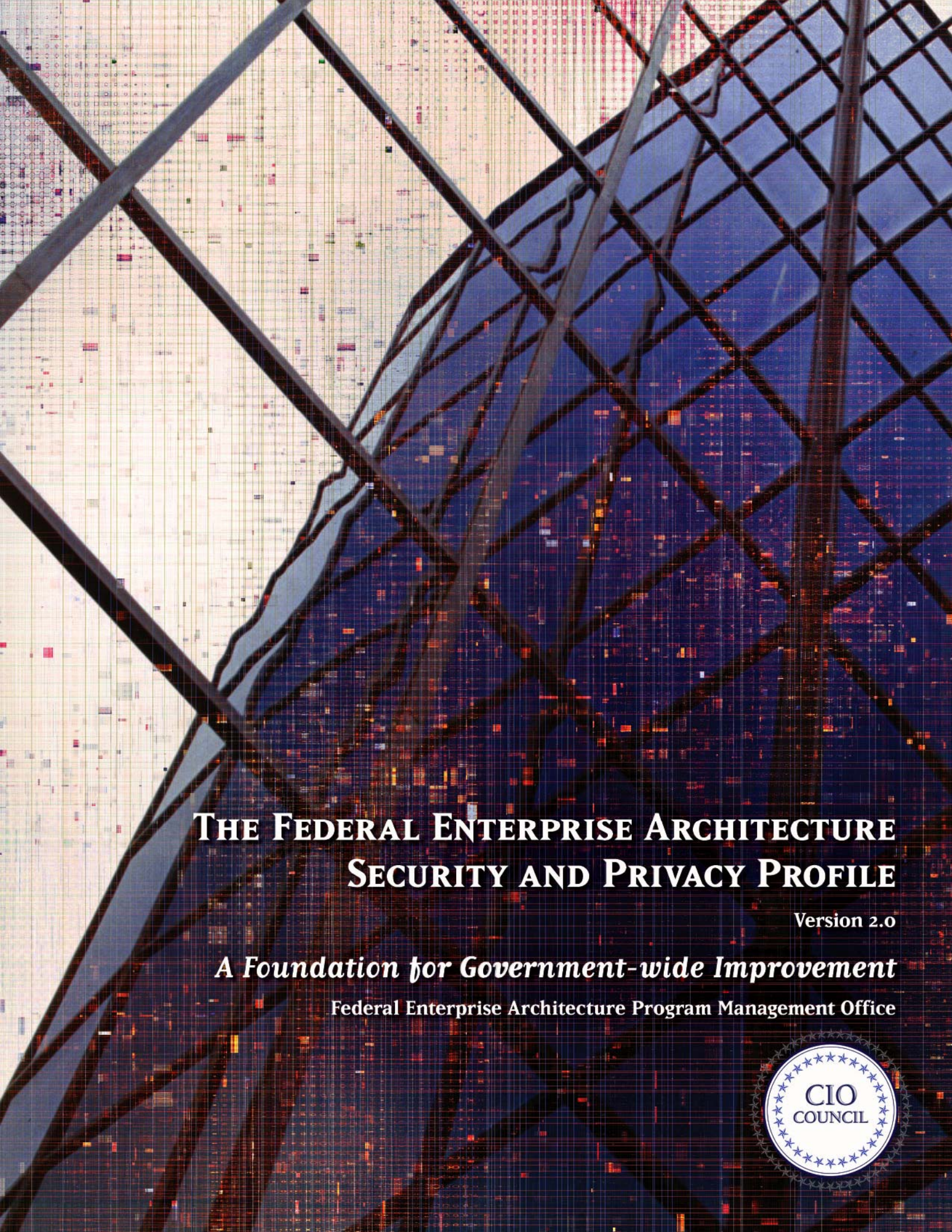

The Federal Enterprise Architecture Security and Privacy Profile

Version 2.0

A Foundation for Government-wide Improvement

Federal Enterprise Architecture Program Management Office

CIO COUNCIL

Contents

1. Chapter One: Introduction 1
   1.1 Target Audience 2
   1.2 Relationship to Other Efforts 2
   1.3 Organization of this Document 4
2. Chapter Two: The Fundamentals 5
   2.1 Enterprise Architecture 5
   2.2 Security 6
   2.3 Privacy 9
   2.4 Security and Privacy 10
   2.5 Capital Planning Perspective on Security and Privacy 11
   2.6 Enterprise Architecture Perspective on Security and Privacy 11
3. Chapter Three: The Methodology 15
   3.1 Stage I – Identification 18
      3.1.1 Introduction 18
      3.1.2 Activities 21
   3.2 Stage II – Analysis 25
      3.2.1 Introduction 25
      3.2.2 Activities 29
   3.3 Stage III – Selection 36
      3.3.1 Introduction 36
      3.3.2 Activities 38
4. Chapter Four: FEA SPP Implementation Over Time 44

Appendix A. References 46
Appendix B. Definitions 48
Appendix C. Acronyms 52
Appendix D. Privacy Requirements 53

Figures

Figure 1. Federal Enterprise Architecture Security and Privacy Profile 1
Figure 2. Federal Enterprise Architecture 3
Figure 3. Process Diagram (Summary) 17
Figure 4. Stage I—Identification 18
Figure 5. Analyze Capabilities 26
Figure 6. Analyze Trade-offs 27
Figure 7. FEA SPP Implementation Level of Effort Over Time 44

Tables

Table 1. FEA SPP Methodology 2
Table 2. Security Control Families 7
Table 3. Privacy Control Families 9
Table 4. FEA Reference Models 13
Table 5. Roles and Responsibilities 15
Table 6. Stage I Activities 21
Table 7. Stage II Activities 29
Table 8. Stage III Activities 38
Table 9. Definitions 48
Table 10. Partial List of Privacy Requirements 53

Document History

The Federal Chief Information Officers Council published initial versions of the Federal Enterprise Architecture Security and Privacy Profile (FEA SPP) in July 2004 and July 2005. The current version of the methodology (Version 2.0) was modified based on validation exercises and an assessment of related documents. Validation testing was conducted at two Federal agencies[1] to verify the methodology's utility. Validation consisted of abbreviated applications of the FEA SPP methodology. An assessment of relatively new standards and documents such as Federal Information Processing Standards Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*; FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*; and Data Reference Model (DRM) Version 2.0 have added to the utility of this document. FEA SPP Version 2.0 supersedes previous FEA SPP releases.

The FEA SPP is voluntary guidance applicable to any Federal government agency; it does not supersede or modify any law, regulation, or executive branch policy. Rather than providing a comprehensive discussion of requirements, the FEA SPP provides best practices and recommendations to promote the successful incorporation of security and privacy into an organization's enterprise architecture and to ensure appropriate consideration of security and privacy requirements in agencies' strategic planning and investment decision processes.

[1] Validation exercises occurred at the Department of Housing and Urban Development and at the Department of Justice between November 2005 and February 2006.

1. Chapter One: Introduction

The Federal Enterprise Architecture Security and Privacy Profile (FEA SPP) is a scaleable and repeatable methodology for addressing information security and privacy from a business-centric enterprise perspective. It integrates the disparate perspectives of program, security, privacy, and capital planning into a coherent process, using an organization's enterprise architecture efforts. Enterprise architecture provides a common language for discussing security and privacy in the context of agencies' business and performance goals, enabling better coordination and integration of efforts and investments across organizational or business activity stovepipes. To support that endeavor, the FEA SPP methodology:

- Promotes an understanding of an organization's security and privacy requirements, its capability to meet those requirements, and the risks to its business associated with failures to meet requirements.
- Helps program executives select the best solutions for meeting requirements and improving current capabilities, leveraging standards and services that are common to the enterprise or the Federal government as appropriate.
- Improves agencies' processes for incorporating privacy and security into major investments and selecting solutions most in keeping with enterprise needs.

As summarized in Figure 1, the FEA SPP evaluates enterprise-level security and privacy in the context of the Federal Enterprise Architecture (FEA). The FEA asks Federal agencies to look at their operations from common business, performance, services, technologies, and data views. Information in those categories is captured in agencies' enterprise architectures to enable enterprise change management by describing how an organization operates today, intends to operate in the future, and intends to invest in technology to transition to that future state. Enterprise architectures are also adapted to reflect the security objectives of confidentiality, integrity, and availability, and the privacy objectives set forth in a variety of Federal laws and regulations.

Figure 1. Federal Enterprise Architecture Security and Privacy Profile

FEA SPP methodology is composed of three stages. Each stage of the methodology includes an introduction of the goals and objectives of that stage and a collection of associated activities that promote completing those goals and objectives. Table 1 introduces the three stages of the FEA SPP methodology and contrasts the FEA SPP's enterprise approach with programmatic approaches.

Table 1. FEA SPP Methodology

Stage	Program Approach	Enterprise Approach
Stage I—Identification	What are my program's needs and capabilities?	How do my program's needs and capabilities relate to those of my agency?
Stage II—Analysis	How can I effectively and cost efficiently address outstanding needs?	Can I reduce costs by leveraging currently deployed Federal agency solutions?
Stage III—Selection	Have I requested adequate funding to accomplish programmatic goals?	Have I requested adequate funding to accomplish mission goals in a manner consistent with my agency's security and privacy requirements? Are security and privacy features of investments coordinated across the organization?

1.1 Target Audience

The FEA SPP is a cross-disciplinary methodology that requires support and participation of experts from security, privacy, enterprise architecture, capital planning, and organizational business functions. It is written at a high level to make it understandable to a wide audience. Success of the FEA SPP methodology hinges on understanding and sharing insights across each domain. Agencies should document those insights in the enterprise architecture and use them to promote the objectives of security and privacy across all enterprise activities and investments. The discussion in Chapter Two introduces basic concepts to facilitate a common understanding of those functional domains.

1.2 Relationship to Other Efforts

The FEA SPP bridges the guidance gap between enterprise architecture and system-level security and privacy activities. The FEA reference models and National Institute of Standards and Technology (NIST) Information Security guidance are two major anchors between which FEA SPP activities take place. The FEA SPP adapts the reference models to use them for describing security and privacy. It also uses outputs from system-level security and privacy activities, aggregating them to present an enterprise picture.

Relationship to FEA Reference Models

The FEA is a business-based framework for government-wide improvement. The goals of the FEA are to locate duplicative investments, discover areas where investments should be made, and identify where departments and agencies can collaborate to

improve government operations or services. Initial FEA efforts involve mapping government operations to five "reference models."

Figure 2 depicts the reference models and demonstrates how these five models interrelate and are mutually supporting. Their purpose is to facilitate cross-agency collaboration that will lead to greater consistency and efficiency in support of citizen-focused delivery of services. While each agency's enterprise architecture will be unique, all agencies' enterprise architectures should map to the five reference models. Chapter Two includes a more specific discussion of the reference models and their relationship to security and privacy. The addition of security and privacy factors is the contribution of the FEA SPP.

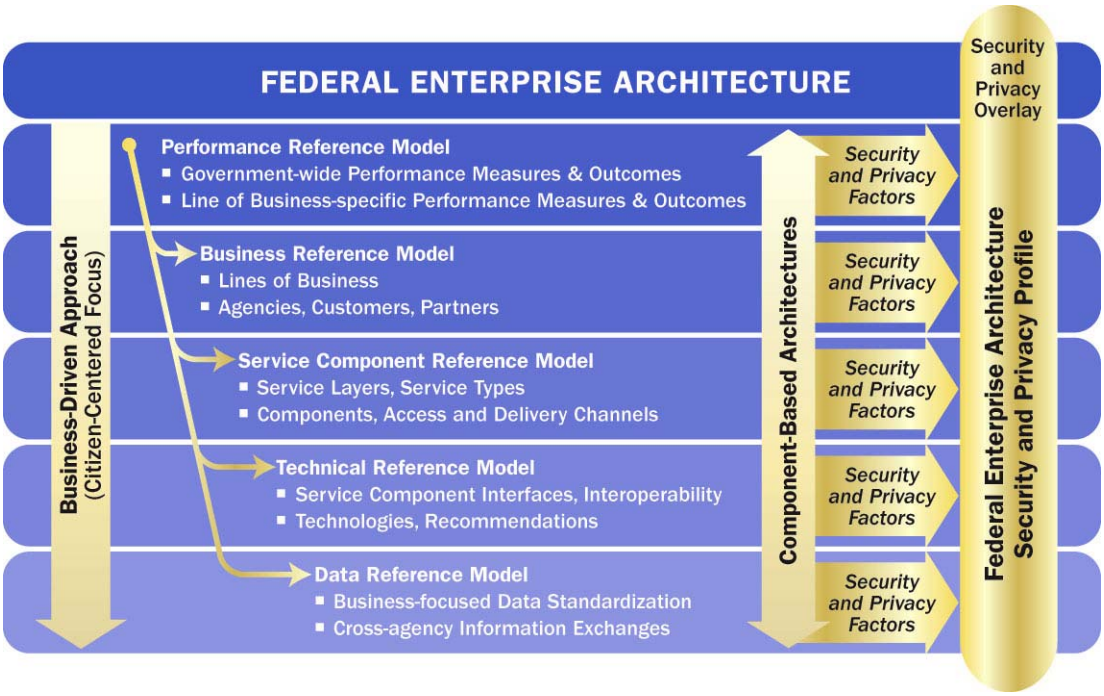

Figure 2. Federal Enterprise Architecture

Relationship to NIST Information Security Standards and Guidance

NIST provides a wide range of information security standards and guidance. The FEA SPP does not replace or alter those documents; it does seek to capture the outputs of system-level security activities and use them to support enterprise decisions. For example:

- An assessment of NIST SP 800-53, *Recommended Security Controls for Federal Information Systems* security baselines contributes to the security requirement identification activity in Stage I.
- The results of Federal Information Processing Standard Publication (FIPS PUB) 199's system-level security categorizations are aggregated in Stage II to identify opportunities to standardize or centralize some security functions.

There is no equivalently rich source of system-level privacy guidance, but the FEA SPP does consider existing guidance concerning system-level privacy activities to support enterprise decision making. It also seeks to add depth to the privacy discussion so that it can be treated equivalently to security.

1.3 Organization of this Document

The remainder of this document is organized as follows:

- **Chapter Two** provides a brief introduction to the functional domains impacted by the FEA SPP methodology: enterprise architecture, security, privacy, and capital planning. It discusses the intersections between those domains and expands on the linkages between the FEA SPP and the FEA reference models. This background supports a common understanding among stakeholders in different functional domains and describes the intersection between those domains.
- **Chapter Three** presents the three-phase FEA SPP methodology. For each stage, an introduction of concepts is followed by a list of activities that support accomplishing the major goals and objectives of that stage.
- **Chapter Four** describes the maturation of FEA SPP efforts over time.

A series of appendices follow the main document:

- **Appendix A** lists cited references.
- **Appendix B** defines terms.
- **Appendix C** lists acronyms.
- **Appendix D** supplies a sample set of privacy requirements.
- **Appendix E** provides a process diagram summarizing the FEA SPP methodology.

2. Chapter Two: The Fundamentals

FEA SPP activities require the active and joint efforts of officials from across an agency. In building a team for FEA SPP implementation, individuals from security, privacy, capital planning, enterprise architecture, and business organizations should be included. Before launching into the FEA SPP methodology, agencies should address two prerequisites. First, it is important to develop a common understanding of the objectives and activities of the methodology. This step should include team members reviewing the FEA SPP and discussing how they will adapt FEA SPP activities to their agency's needs and enterprise architecture. Second, team members need to gain a basic understanding of each participant's functional domain. Likewise, team members should work with program officials to gain an understanding of agency business goals. Chapter Two addresses these needs; representatives of the various functional domains should relate Chapter Two's generic descriptions to actual practices within an agency.

This chapter serves as a brief introduction to enterprise architecture, security, and privacy. It also provides an overview of the intersections between:

- Security and Privacy
- Security, Privacy, and Capital Planning
- Security, Privacy, and Enterprise Architecture

2.1 Enterprise Architecture

Enterprise architecture is a technique for documenting, evaluating, and planning an organization's business objectives and the business activities, information, standards, and capabilities that support those objectives.[2] Agencies typically maintain two versions of their enterprise architecture. The version that portrays the existing enterprise, the current business practices and the associated technical infrastructure is defined as a *baseline* or *as-is* architecture. The as-is architecture can be used to reduce costs and increase interoperability by helping organizations become aware of and reuse existing assets and develop enterprise solutions with reuse and interoperability in mind. Understanding and establishing reusable components is an integral part of continuously improving an organization's IT portfolio management.[3]

The enterprise architecture also describes the desired future state for an organization—called the *target* or *to-be* architecture. Like the *as-is* architecture, the *to-be* architecture defines business objectives and supportive activities in both business and technical

---

[2] *A Practical Guide to Federal Enterprise Architecture* defines enterprise architecture as "a strategic information asset base, which defines the mission, the information necessary to perform the mission, and the transitional processes for implementing new technologies in response to the changing mission needs."

[3] Government Accountability Office (GAO) Report: Practical Guide to Federal Enterprise Architecture – Chief Information Officer Council Version 1.0 February 2001. http://www.gao.gov/bestpractices/bpeaguide.pdf

terms. Organizations move from the baseline state to the target state through a *sequencing* or *transition* plan.

There are many approaches to modeling the current and future states of an enterprise. Federal agencies are free to select any approach; however, all Federal agency enterprise architectures must map to the Federal Enterprise Architecture's five reference models.[4] This mapping facilitates cross-agency analysis and identification of gaps, duplicative investments, and opportunities for collaboration within and across agencies.

The reference models are used to better understand current organizational activities and capabilities by describing them in standard terms that are recognized across the Federal government. As a result, personnel planning new programmatic or technical capabilities can understand issues such as specific business-related performance objectives, the technical infrastructure in which technologies will be deployed, and the data processed by the enterprise. By understanding such issues, new capabilities may better compliment and integrate with existing needs and capabilities. Key results include reducing integration costs and avoiding unnecessarily duplicative spending. Applying enterprise architecture principles to existing investments helps identify previously undetected efficiencies.

2.2 Security

The Federal Information Security Management Act (FISMA) of 2002 is the primary legislation driving Federal agencies' information security activities. Designed around accountability, FISMA sets forth specific security activities and associated reporting requirements. Implementation of FISMA occurs through the Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources* (OMB A-130), and through NIST guidance.

Generally, information security describes the activities that assure the confidentiality, integrity and availability of information and information systems.

- Confidentiality refers to understanding which data may and may not be disclosed to which people and ensuring that only appropriate disclosures are made.
- Integrity is the assurance that information and information systems are protected against improper or accidental modification.
- Availability is assurance of timely and reliable access to information and information systems by authorized persons.[5]

---

[4] For detailed information about the Federal Enterprise Architecture reference models, visit http://www.whitehouse.gov/omb/egov/.

[5] FISMA defines integrity, confidentiality, and availability as follows: (A)integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (C) availability, which means ensuring timely and reliable access to and use of information.

FISMA mandates a risk-management approach to securing Federal information and information systems. Each Agency Head is responsible for "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction"[6] of agency information and information systems. The FEA SPP helps meet that requirement, and also the requirement that each Agency Head has responsibility for "ensuring that information security management processes are integrated with agency strategic and operational planning processes."[7]

Federal agencies achieve confidentiality, integrity, and availability, and the associated FISMA goals through applying safeguards and countermeasures (controls). Seventeen categories (families) of managerial, operational, and technical controls support achieving appropriate confidentiality, integrity, and availability (see Table 2).[8] Agencies' information security officials identify the appropriate set of controls from each control family through categorizing each information system; they categorize systems based on the potential impact of a loss based on the data they contain.[9] Among other activities, the FEA SPP describes how enterprise decision-makers can take advantage of the aggregated results of this system-level categorization.

Table 2. Security Control Families

Security Control Family	Description
Risk Assessment	Assessing the risk to organizational operations, assets, and individuals resulting from the operation of information systems, and the processing, storage, or transmission of information.
Planning	Developing, documenting, updating, and implementing security plans for systems.
System and Services Acquisition	Allocating resources to protect systems, employing system development life cycle processes, employing software usage and installation restrictions, and ensuring that third-party providers employ adequate security measures to protect outsourced information, applications, or services.
Certification and Accreditation and Security Assessments	Assessing security controls for effectiveness, implementing plans to correct deficiencies and to reduce vulnerabilities, authorizing the operation of information systems and system connections, and monitoring system security controls.

6 FISMA

7 Ibid.

8 NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, February 2005. (SP 800-53)

9 FIPS PUB 199 requires describing each system in terms of a low, moderate, or high impact to an agency's business following a breach of confidentiality, integrity, or availability.

Security Control Family	Description
Personnel Security	Ensuring that individuals in positions of authority are trustworthy and meet security criteria, ensuring that information and information systems are protected during personnel actions, and employing formal sanctions for personnel failing to comply with security policies and procedures.
Physical and Environmental Protection	Limiting physical access to systems and to equipment to authorized individuals, protecting the physical plant and support infrastructure for systems, providing supporting utilities for systems, protecting systems against environmental hazards, and providing environmental controls in facilities that contain systems.
Contingency Planning	Establishing and implementing plans for emergency response, backup operations, and post-disaster recovery of information systems.
Configuration Management	Establishing baseline configurations and inventories of systems, enforcing security configuration settings for products, monitoring and controlling changes to baseline configurations and to components of systems throughout their system development life cycles.
Maintenance	Performing periodic and timely maintenance of systems and providing effective controls on the tools, techniques, mechanisms, and personnel that perform system maintenance.
System and Information Integrity	Identifying, reporting, and correcting information and system flaws in a timely manner, providing protection from malicious code, and monitoring system security alerts and advisories.
Media Protection	Protecting information in printed form or on digital media, limiting access to information to authorized users, and sanitizing or destroying digital media before disposal or reuse.
Incident Response	Establishing operational incident handling capabilities for information systems and tracking, documenting, and reporting incidents to appropriate officials.
Awareness and Training	Ensuring that managers and users of information systems are made aware of the security risks associated with their activities and of applicable laws, policies, and procedures related to security and ensuring that personnel are trained to carry out their assigned information security-related duties.
Identification and Authentication	Identifying and authenticating the identities of users, processes, or devices that require access to information systems.
Access Control	Limiting information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems), and to types of transactions and functions that authorized users are permitted to exercise.
Audit and Accountability	Creating, protecting, and retaining information system audit records that are needed for the monitoring, analysis, investigation, and reporting of unlawful, unauthorized or inappropriate information system activity, and ensuring that the actions of individual users can be traced so that the individual users can be held accountable for their actions.

Security Control Family	Description
System and Communications Protection	Monitoring, controlling and protecting communications at external and internal boundaries of information systems, and employing architectural designs, software development techniques, and systems engineering principles to promote effective security.

2.3 Privacy

The Privacy Act of 1974 (Privacy Act) stands as the landmark in Federal privacy legislation, influencing nearly all privacy laws and guidance that came after it. More recently, the E-Government Act of 2002 (E-Gov Act) and associated guidance has had a significant impact on privacy, creating a risk-based decision-making process for addressing privacy requirements. OMB provide specific guidance on the implementation of each of these acts, much of it consolidated in Memorandum 03-22; however, OMB also has specific guidance on the implementation of the Privacy Act and agency responsibilities for protecting privacy. The inclusion of privacy in FISMA reporting highlights specific areas of prioritization at the agencies including Privacy Act reviews, system of record notices, roles and responsibilities, and training programs. This has raised the visibility of privacy at federal agencies.

The FEA SPP defines 17 privacy control families (see Table 3). These control families provide a common terminology and framework for privacy controls in a manner similar to the 17 security control families defined in NIST SP 800-53. These control areas are common across most privacy laws and provide a framework for organizing and addressing privacy requirements and capabilities.

Most privacy controls have both a system and enterprise aspect. Like security, privacy can be very system-focused. For example, conducting system-level privacy impact assessments (PIA) to assess system-related information privacy practices and determine compliance, risks, and safeguards has been a major focus for agencies. Individual PIAs can provide insight into the need for and performance against privacy control families. Evaluating PIAs across an enterprise can identify aggregated privacy weaknesses to support enterprise-level decision-making.

Table 3. Privacy Control Families

Privacy Control Family	Description
Policies and Procedures	Creating policies and procedures governing the appropriate use of personal information and implementing privacy controls.
Privacy as Part of the Development Life Cycle	Implementing privacy reviews and controls throughout the system development life cycle.
Assigned Roles, Responsibilities, and Accountability	Identifying general and specific roles and responsibilities for managing and using personal information and ensuring accountability for meeting these responsibilities.
Monitoring and Measuring	Monitoring the implementation of privacy controls and measuring their efficacy.

Privacy Control Family	Description
Education: Awareness and Role-based Training Programs	Ensuring managers and users of personal information are made aware of the privacy risks associated with their activities and of applicable laws, policies, and procedures related to privacy.
Public Disclosure	Publicly disclosing privacy policies and procedures for a program or system.
Notice	Providing notice of the information practices to the individual before collecting personal information.
Consent	Gaining consent from the individual to use their personal information.
Minimum Necessary	Collecting the minimum amount of personal information necessary to accomplish the business purpose.
Acceptable Use	Ensuring that personal information is used only in the manner provided on the notice, to which the individual consented, and in accordance with the publicly disclosed practices.
Accuracy of Data	Ensuring that personal information is accurate, particularly if harm or denial of benefits may result.
Individual Rights	Providing individuals an opportunity to access and correct their personal information and to seek redress for privacy violations.
Authorization	Ensuring that the individual authorizes all new and secondary uses of personal information not previously identified on the original collection notice.
Chain of Trust	Establishing and monitoring third-party agreements for the handling of personal information.
Risk Management	Assessing and managing risks to operations, assets, and individuals resulting from the collection, sharing, storing, transmitting, and use of personal information.
Reporting and Response	Providing senior managers and oversight officials the results of the monitoring and measuring of privacy controls and responding to privacy violations.
Security Measures	Implementing the appropriate safeguards to assure confidentiality, integrity and availability of personal information.

2.4 Security and Privacy

While they are unique disciplines, security and privacy share some commonalities. Once personal information is collected, security measures are crucial to assuring privacy. The FEA SPP will help identify areas where considering security and privacy together can yield efficiencies. For example, both security and privacy have controls for education and awareness, and agencies may choose to implement security and privacy education programs together. However, it is important to note that privacy is more complex than just an application of security. The privacy control families listed in Table 3 include several topics that may be unfamiliar to security professionals, including public disclosure, notice, and consent.

Nevertheless, assuring security and privacy often falls on the same people. The FEA SPP is consistent with the frequently observed pattern of considering security and privacy together. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) features both security and privacy rules; the capital planning process requires an accounting of security and privacy controls and costs; and under FISMA, OMB collects both security and privacy performance data.

2.5 Capital Planning Perspective on Security and Privacy

Capital planning refers to an agency's planned budget execution strategy. The capital planning process of today is driven by the Clinger Cohen Act of 1996[10]. The Clinger Cohen Act assigns overall responsibility for the acquisition and management of federal information technology investments to OMB. It also gives authority to acquire IT resources to the head of each executive agency and makes them responsible for effectively managing their IT investments. Most importantly from a capital planning perspective, it requires agencies to base IT investment decisions on quantitative and qualitative factors associated with the costs, benefits, and risks of those investments and to use performance data to demonstrate how well the IT expenditures support improvements to agency programs. To accomplish these goals, the act requires agencies to appoint CIOs to carry out the IT management provisions of the act and the broader information resources management requirements of the Paperwork Reduction Act.

Office of Management and Budget Circular A-11, *Preparation, Submission, and Execution of the Federal Budget* (OMB A-11), provides federal agencies with guidance on how to prepare, submit, and execute their budgets in accordance with the Clinger Cohen Act and the Federal Acquisition Streamlining Act of 1994 (FASA). OMB A-11 directs agencies to complete Exhibit 300s and Exhibit 53s. The Exhibit 300 reflects investment-related plans for capital asset management. In addition, the Exhibit 300 guidance instructs agencies on budget justification and reporting requirements for major acquisitions and major IT systems or projects. The Exhibit 300 is an input to the Exhibit 53, which provides the total IT and information security spending for the year.

The Clinger Cohen Act, FISMA, and other federal requirements charge agencies with integrating capital planning and security activities. Within each Exhibit 300, agencies must report on how the IT investment satisfies federal security and privacy requirements. In making funding decisions, OMB assesses how well security and privacy details of the investment are documented and budgeted for throughout the proposed investment life cycle.[11]

2.6 Enterprise Architecture Perspective on Security and Privacy

Linking security and privacy to the agency enterprise architecture has two major benefits:

---

[10] Formerly known as the Information Technology Management Act of 1995.

[11] OMB evaluates Exhibit 300s against several criteria in addition to security and privacy. For more details see section 3.3.1 of this document.

- Layering security and privacy over agency performance objectives, business processes, service-components, technologies, and data helps ensure that each aspect of the business receives appropriate security and privacy attention.
- Describing security and privacy using enterprise architecture reference models promotes interoperability and aids in standardizing and consolidating security and privacy capabilities as appropriate.

Enterprise architecture discussions of security and privacy span two types of capabilities. In some instances security or privacy features may be inherent in a particular asset (such as the security features built into a web server) or part of a particular service (the web security and privacy policy for an e-Gov initiative). In other instances, security or privacy are the primary objectives of a capability—for example, an Internet firewall protecting an organization's web site. Agency enterprise architectures must capture information about both types of capabilities and document their security and privacy features across each reference model. Doing so enables agencies to better understand and align security and privacy activities to the business and performance objectives of the organization. Additionally, effectively representing security and privacy information in the enterprise architecture ensures that security and privacy are adequately included in the life cycle processes of the agency.

Table 4 describes the five reference models and suggests how agencies may wish to document security and privacy in their enterprise architectures. As agencies capture security and privacy features in their enterprise architectures, they will be able to identify unmet requirements, determine what capabilities may be improved, and make strategic decisions that are best for the enterprise as a whole.

Table 4. FEA Reference Models[12]

Reference Model	Description
Performance Reference Model (PRM)	Information in the PRM helps agencies understand how well they are accomplishing business goals and objectives. The PRM includes a compilation of performance objectives and the performance metrics used to monitor business activity progress. Laws and regulations establish many of these objectives and metrics. Agencies will also develop their own specific objectives and metrics. The PRM should contain documentation of all business-related performance objectives and performance metrics. By compiling this information and using it to support decision-making and process improvement efforts, agencies can identify improved service-delivery approaches, improve underperforming programs, and leverage existing performance management tools across the entire Federal government. The Security and Privacy category falls under PRM Measurement Area "Process and Activities." Measurement Indicators show the extent to which security is improved and privacy addressed. Examples of security and privacy indicators from the FY05 FISMA report include: ▪ Percentage of employees who received annual security awareness training ▪ Percentage of agency websites with a machine-readable privacy policy ▪ Percentage of systems with certification and accreditation ▪ Percentage of applicable systems with a privacy impact assessment.
Business Reference Model (BRM)	Information in the BRM helps agencies understand their primary business functions and the processes that support them. The BRM breaks down the basic types of services that an agency provides to the American public and identifies the methods and support services employed to deliver those services and the mission of the department. The BRM identifies four business areas, 39 lines of business and 153 sub-functions for government services. Agencies describe their business activities using this taxonomy. For example, an agency may provide a (1) service to citizens (2) in the Community and Social Services line of business (3) under the Homeownership Promotion sub-function. Business-specific processes would be enumerated under each sub-function. Various lines of business, sub-functions, and processes are exposed to different types and levels of security and privacy risk. Also, "Security and Privacy" is a support activity that falls under the "Management of Government Resources" Business Area. Various aspects of security and privacy will fall under the Information and Technology line-of-business and Administrative line-of-business. Sub-functions include IT Security and Security Management.
Service-Component Reference Model (SRM)	The SRM helps agencies document business and performance-supportive capabilities. These capabilities in a department will map to seven service domains and service types within these domains. By understanding and similarly classifying capabilities, agencies will more easily support the discovery of government-wide business and application Service Components in IT investments and assets. Non-security and non-privacy capabilities may have security or privacy features. Most security-specific capabilities will be located under the Service Domain "Support Services" under the Service Type, "Security Management." "Audit Trail Capture and Analysis" is an example of a Service Capability within Security Management.

[12] Official definitions and descriptions of the FEA reference models are available from OMB's *FY07 Budget Formulation: FEA Consolidated Reference Model Document,* May 2005.

Reference Model	Description
Technology Reference Model (TRM)	The TRM helps agencies document technologies and standards used to support the service components. It provides a component-driven, technical framework that categorizes the standards and technologies to support and enable the delivery of Service Components and capabilities. It also provides a foundation to advance the reuse and standardization of technology and service components from the agency and government-wide perspectives Service areas include Service Access and Delivery, Service Platform and Infrastructure, Component Framework, and Service Interface and Integration. Security is a category under the Component Framework; however, an agency TRM will likely reference security and privacy in several areas. For example, "Data Types/ Validation" is under Service Interface and Integration/ Interoperability. The data types may determine unique security and privacy requirements.
Data Reference Model (DRM)	The DRM asks: What data and information does the Department have to support the business objectives? The DRM helps agencies describe their data at an aggregate level and enables agencies to describe the types of interaction and exchanges occurring among Federal agencies and citizens. Currently, the DRM standardizes three aspects of data management: ▪ Data Description: Provides a means to uniformly describe data, thereby supporting its discovery and sharing ▪ Data Context: Facilitates discovery of data through an approach categorizing data according to taxonomies; additionally, enables the definition of authoritative data assets within a community of interest ▪ Data Sharing: Supports the access and exchange of data where access consists of ad-hoc requests (such as a query of a data asset) and exchange consists of fixed, re-occurring transactions between parties Data described, contextualized and shared through the DRM may include personal information and/or proprietary information that will trigger security and privacy requirements. For example, data sharing involving social security numbers may require chain of trust agreements.

Security and privacy are reflected in each reference model, but the level of description varies greatly between reference models. As OMB reviews security and privacy features in agency enterprise architectures, common taxonomies will evolve. For example, the BRM does not currently describe security activities more deeply than the sub-function of IT security management. Additionally, only the PRM explicitly identifies privacy. However, agencies will still need to capture security and privacy to fully support the agency enterprise architecture goals. For example, despite the lack of granularity regarding security, agency enterprise architectures should capture business processes supporting the IT Security sub-functions. As agencies describe these processes, OMB may identify security and privacy with greater granularly in the BRM.[13]

[13] *Federal Enterprise Architecture Reference Model Maintenance Process*, Chief Information Officer Council, et. al., June 2005.

3. Chapter Three: The Methodology

The FEA SPP will be most useful when used as a guide for discussion between business and functional stakeholders. Activities described in Table 5 are an opportunity for awareness and interaction between stakeholders that promote a more coordinated approach to security and privacy consistent with agencies' business objectives and the goals of efficiency and interoperability.

Using this methodology requires the coordinated efforts of business leaders and functional domain experts, including security, privacy, enterprise architecture, and capital planning. By working together, these people enable business transformation. Agencies may wish to consider inclusion of other key stakeholders who can make significant contributions to the methodology, such as representatives of the acquisitions, contracts, and legal departments. Ideally, implementing the FEA SPP includes the officials listed in Table 5.

Table 5. Roles and Responsibilities

Roles	Responsibilities
Chief Information Officer (CIO)	The CIO is responsible for information resource management and will be a natural stakeholder for the FEA SPP methodology.
Senior Agency Official for Security	The senior agency official for security has primary responsibility for security in the agency and should be familiar with external and internal security requirements as well as the enterprise-level capabilities currently in place to satisfy those requirements. The senior agency official for security also contributes knowledge of the organization's current security posture. More than one security official may be needed to support the FEA SPP methodology in agencies where security responsibilities are decentralized.
Senior Agency Official for Privacy	The senior agency official for privacy has primary responsibility for privacy in the agency and should be familiar with external and internal privacy requirements as well as the enterprise-level capabilities currently in place to satisfy these requirements. The senior agency official for privacy also contributes knowledge of the organization's current privacy posture. Privacy may have several advocates within an agency.
Chief Enterprise Architect	The Chief Enterprise Architect has primary responsibility for developing and promoting the operationalization of the enterprise architecture of an organization. In light of those responsibilities, the Architect may be the best person to lead FEA SPP activities and to capture outcomes.
Chief Financial Officer (CFO)	The CFO has responsibility for planning, proposing, and monitoring major agency investments. The CFO is also often the chair of agencies' information technology investment review boards (ITIRB). The FEA SPP's goal of promoting better-informed and more strategic investment decisions makes it important that the CFO participates in this process, especially with regard to Stage III's activities. By following the guidance in the FEA SPP, an organization is more likely to effectively address security and privacy requirements in Exhibit 300 and Exhibit 53 submissions.

Roles	Responsibilities
Program Officials	Program officials are responsible for accomplishing the business of an agency. They drive decisions about investments and are responsible for planning and budgeting for security and privacy. While security and privacy officials will be knowledgeable about enterprise security and privacy requirements, program officials may have unique, programmatic requirements. Also, senior agency officials' decisions in the course of developing the FEA SPP will impact the program-level as the program officials will implement many of the security and privacy decisions. Including program officials in the FEA SPP activities will ensure that decisions made will be practical and useful to everyone.

The list of roles presented in Table 5 is not exhaustive. Agency officials may wish to expand this list to meet specific needs. The methodology discussions include activities that may benefit from other agency officials' inputs.

Additional considerations for agency officials include establishing a formal governance process or leadership structure when initiating FEA SPP activities. Additionally, agency officials may want to review the stages of the methodology to gain a common understanding of the goals, objectives, and activities among all team members. Team members can help translate some of the generic terms of the FEA SPP into the language of the agency.

The remainder of Chapter Three details the three stages of the FEA SPP methodology (Figure 3 is a summary of the methodology). Each stage includes an introduction of the goals and objectives of that stage, and a table of associated activities that promote the accomplishment of those goals and objectives. The table facilitates documenting FEA SPP-supportive information sources, or gaps in the required information. When completed, this table will be an initial output of the FEA SPP methodology, providing a valuable feed to the agency's enterprise architecture. However, readers should note that the heart of the FEA SPP is the subsequent application of the documented information to support security and privacy-supportive enterprise change.

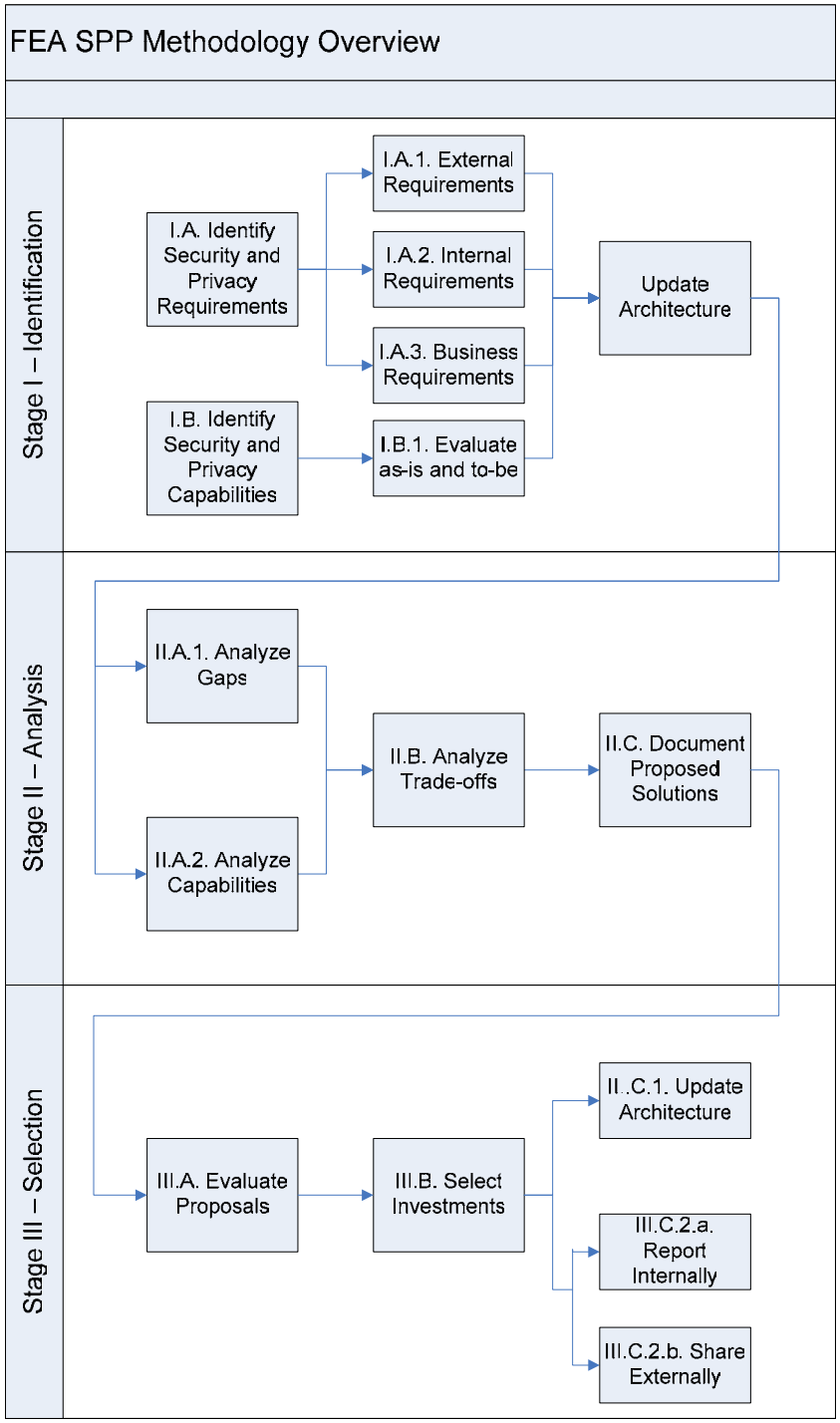

Figure 3. Process Diagram (Summary)

3.1 Stage I – Identification

3.1.1 Introduction

Stage I is an identification of an agency's business-supportive security and privacy requirements and the existing or planned capabilities that support security and privacy (see Figure 4). As a result of Stage I activities an agency will be able to:

- Fully identify program and enterprise-level security and privacy requirements, including previously unknown requirements.
- Fully identify program and enterprise-level security and privacy capabilities, including current and planned future requirements.
- Document requirements and capabilities in an agency's enterprise architecture using a nomenclature that is common across the Federal government.

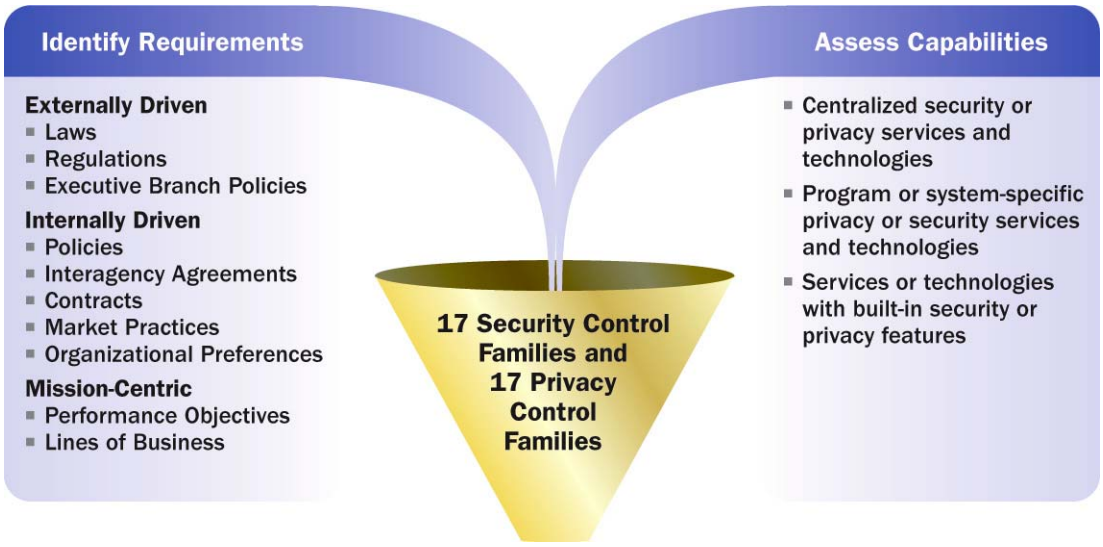

Figure 4. Stage I—Identification

To accomplish those goals, agencies may wish to evaluate three types of requirements:

- Externally driven laws, regulations, and executive branch policies;
- Internally driven policies, interagency agreements, contracts, market practices, and organizational preferences; and
- Mission-centric drivers such as performance objectives and lines of business.

Agencies may also wish to evaluate three types of capabilities:

- Centralized security or privacy services and technologies,
- Program or system-specific security or privacy services and technologies; and
- Services or technologies with built-in security or privacy features.

Consistent with OMB requirements,[14] the FEA SPP encourages requirement and capability documentation to help assess enterprise risk by gaining a view of threats and vulnerabilities as documented and acknowledged by the enterprise. Agencies develop requirement documents—especially the internally driven requirement documents—with an eye towards addressing programmatic and enterprise-level threats. Similarly, agencies select security and privacy-supportive capabilities to mitigate vulnerabilities. These perspectives on agencies' risk mitigation needs and activities contribute to the analyses in Stage II.

Once identified, agencies will update their enterprise architectures to reflect the requirements and capabilities. Consider, for example, that the E-Gov Act requires that agencies conduct PIAs. Agencies will document the mandated frequency and scope of PIAs in the PRM while capturing the business processes used to conduct PIAs in the BRM. Agencies will document the standards and templates supporting PIAs in the TRM while associating data elements with privacy-related considerations in the DRM. Finally, agencies will document the capabilities that support PIAs in the SRM.

Chapter Two introduced a common set of security and privacy control families to enable a consistent description of security and privacy requirements and capabilities across the enterprise. Each security and privacy requirement maps to a control family; each security and privacy capability maps to one or more control families. This common terminology for security and privacy helps to ensure consistent expression of the information from the FEA SPP analysis and consistent documentation in agency enterprise architectures. Using consistent and common language to describe security and privacy requirements and capabilities helps agencies promote collaboration across the Agency and across the Federal government (see Stages II and III).

Agencies can take a top-down or bottom-up approach to Stage I. The FEA SPP recommends a top-down approach in which the high-level requirement and capability identification begins at the enterprise level. Results from that activity are then available to a line of business or more specific program or system for customization. The advantage of this approach is that agencies capture common requirements once, reducing the difficulty of programmatic efforts. Additionally, a top-down approach helps ensures an enterprise-centric application of the FEA SPP rather than a stove-piped point of view. Adopting an enterprise-centric point of view is consistent with OMB's FEA guidance.[15]

However, the programmatic activities have the greatest and most immediate need for Stage I activities; this is especially the case when agencies are creating new programs and systems. Funding to support the FEA SPP may be more readily available through agency programs. Therefore, some organizations may launch Stage I activities in a

---

[14] OMB A-130 requires that agencies implement enterprise architectures in a manner that supports "[Establishing] a level of security for all information systems that is commensurate to the risk and magnitude of the harm resulting from the loss, misuse, unauthorized access to, or modification of the information stored or flowing through these systems."

[15] *FY07 Budget Formulation: FEA Consolidated Reference Model Document*, OMB, May 2005.

bottom-up approach. In those cases the first completed programmatic effort can serve as a model for others. Stage I accommodates either approach.

Regardless of the chosen approach, Stage I activities are best accomplished with the participation of as many of the key contributors as possible. The difference between top-down and bottom-up approaches will be in the breadth of functional and program official participation. This is important because much of the needed content may already exist in some form or another and may be possessed and maintained by one or more contributors.

After identifying security and privacy requirements and capabilities, agencies can evaluate them against the *as-is* and *to-be* architectures to ensure that these requirements and capabilities are adequately represented and supported by the enterprise architecture. Stage II will introduce approaches for analyzing the outputs of Stage I, leading to proposed additions to or changes in agencies' security or privacy capabilities. Specifically, Stage I activities immediately enable agencies to improve operations by:

- Analyzing gaps between requirements and capabilities to identify unmet requirements
- Analyzing their portfolio of current capabilities (an as-is security and privacy architecture) to identify opportunities to increase interoperability and standardization, and reduce costs
- Proposing future capabilities based on improved insights into the enterprise
- Facilitating enterprise-level choices about the implication of security and privacy decisions and investments.

3.1.2 Activities

The following activities support the goals and objectives of Stage I. For each activity, security and privacy information for the enterprise and/or program should be integrated into the agency's enterprise architecture. The following table provides a tool to determine where activities' outputs should be documented, identify the location where data is maintained, identify the owners of associated data, and document any corrective actions identified to improve the data or complete the activity.

Table 6. Stage I Activities

Goals, Objectives, Activities	EA Component	Information Location	Information Owner	Issues
A. 1. architecture. Security and privacy-related business processes should be highlighted in the agency's business architecture. System components providing security and privacy capabilities should be highlighted in the agency's system architecture. A clear understanding of performance requirements is the first step toward risk-management and compliance. An understanding of security and privacy requirements can be derived from business-specific documents as well as from security and privacy-specific documents.				
a. Identify those laws, regulations, and executive branch policies that establish business requirements.	Drivers[16]			
b. Identify those laws, regulations, and executive branch policies that establish security and privacy requirements.				
i. privacy. Security examples include FISMA, OMB A-130, FIPS PUB 199, FIPS PUB 200, and others. Some privacy examples are cited in Appendix D.	Drivers			

[16] Organizations should capture external, internal, and business requirements in their enterprise architectures. The location for that information will vary based on the specific structure of an agency's enterprise architecture and may not be captured in any particular reference model.

Goals, Objectives, Activities	EA Component	Information Location	Information Owner	Issues
ii. Evaluate key requirements for system-level security and privacy. NIST captures system-level security requirements in the NIST SP 800-53 baseline security controls. Primary sources of enterprise requirements include sources such as FISMA, OMB A-130, FIPS PUB 199, and FIPS PUB 200.	Drivers			
2. insights into security and privacy needs and should be reflected explicitly in the enterprise business architecture. While many internal requirements are entered into voluntarily, it remains critical to be aware of and compliant with these requirements while they are in effect. a. Identify security and privacy requirements established in agency or organizational mission statements and policies. The ability to link security and privacy capabilities to policy and strategy ensures alignment of security and privacy capabilities with the business mission.[17]	Drivers			
b. Document security and privacy roles and responsibilities in relevant policies and position descriptions. Establishing accountability reduces the risks regarding the appropriate and consistent application of security and privacy controls.	Baseline[18]			
c. Identify security and privacy commitments established through inter and intra-agency trust agreements and contracts. Evaluate whether those commitments have programmatic or enterprise-wide impact on security and privacy.	Drivers			
d. Identify and document security and privacy practices driven by organizational preferences and market practices. Evaluate the criticality of non-mandatory practices in terms of risk and cost.	Drivers			

[17] This activity assumes that agencies' internal requirement documents reflect an adequate assessment of the threats to and vulnerabilities of agency information and information systems in a manner that addresses enterprise security and privacy risks. Future ISO/IEC Standard 27005, *Information Security Management System Risk Management* will address approaches for enterprise risk assessment.

[18] "Baseline" is the *as-is* architecture.

Goals, Objectives, Activities	EA Component	Information Location	Information Owner	Issues
3. Identify Business Requirements. These include performance, business, and data requirements. a. Assess enterprise architecture descriptions of performance objectives to determine if they support measuring compliance. In addition to compliance oversight, metrics should also assess adequacy of performance and support service-level agreements.				
i. Stage I requirement (those identified in activities 1 and 2 above).	PRM			
ii. 55 or a comparable agency methodology.	PRM			
b. Assess enterprise architecture descriptions of lines of business, functions, and sub-functions to determine if they describe security and privacy attributes. The business architecture should highlight security and privacy-sensitive activities to each business function and sub-function to ensure that appropriate controls are developed and in place.	BRM			
c. Ensure that enterprise architecture descriptions of data incorporate security and privacy attributes. i. information confidentiality, integrity, and availability. FIPS PUB 199 and NIST SP 800-60 describe the methodology for this activity. This guidance helps agencies map security impact levels in a consistent manner to types of information (e.g., privacy, medical, proprietary, financial, contractor sensitive, trade secret, investigation) and information system (mission critical, mission support, administrative).	DRM			
ii. subject to privacy legislation. Especially consider the Privacy Act, eGov Act, and HIPAA.	DRM			
iii. must be associated with a business purpose to properly assess associated risks.	DRM, BRM			

Goals, Objectives, Activities	EA Component	Information Location	Information Owner	Issues
Identify Security and Privacy Capabilities 1.				
a. Identify processes and technologies that provide dedicated security or privacy services—for example, processes for managing classified information, or a stand-alone Internet firewall or a web-based PIA tool.	BRM, TRM			
b. Identify processes and technologies that are not security or privacy-centric but which accomplish security or privacy as an ancillary function—for example, personnel management activities that require consideration for privacy, or a grants-management system that encrypts data.	BRM, TRM			
2. by how it supports one or more of the 17 security and 17 privacy control families. The controls families will be used in Stage II to map requirements to capabilities and identify gaps. Incorporate information about security and privacy capabilities into the agency's *as-is* architecture. Security and privacy-related business processes should be highlighted in the agency's business architecture. System components providing security and privacy capabilities should be highlighted in the agency's system architecture.	SRM, TRM			

3.2 Stage II – Analysis

3.2.1 Introduction

In Stage II agencies analyze their business-supportive security and privacy requirements and the existing or planned capabilities that support security and privacy. Stage II's three analyses help agencies:

- Identify gaps between requirements and current or planned capabilities.
- Identify opportunities to increase interoperability between or reduce costs of current or planned capabilities.
- Propose solutions to address gaps or improve capabilities based on an informed trade-off analysis of alternatives.

The first analysis is the discovery of gaps between requirements and capabilities. When considered from an enterprise risk perspective, a gap between requirements and capabilities is the failure to address a documented security or privacy need. In Stage I, agencies identify and map requirements and capabilities to the enterprise architecture and control families. The Stage II gap analysis is a natural output of Stage I identification activities. Consider this example:

- In Stage I an agency identifies the FISMA requirement to conduct security awareness training. The FEA SPP team documents this requirement in the enterprise architecture and maps it to the "awareness and training" security control family. The agency also identifies two security-related awareness training capabilities. These may include a computer-based training course on password protection and a classroom-based course on configuring security firewalls. The FEA SPP team documents these capabilities in the SRM and maps them to the "awareness and training" security control family. The agency also determines that there are no awareness and training-related investments documented in the *to-be* architecture.
- In Stage II the FEA SPP team works through each control family, comparing each requirement in a family to available components. They note as gaps those requirements that are not satisfied by an existing component. In this example, an agency is likely to determine that no agency capability fully supports the FISMA requirement to conduct security awareness training—a gap has been identified.

The second analysis supports optimizing security and privacy capabilities. This optimization promotes improved security and privacy functionality, increased standardization and interoperability, and reduced risk. Historically, agencies selected capabilities based on programmatic needs. They may not have considered the impact of local choices on the broader enterprise's security and privacy posture; or the environment may have changed, leading to unexpected impacts that increase risk to part or all of an enterprise. Similarly, agencies may not have considered the opportunities for savings inherent in building interoperable or standardized capabilities. Agencies document standards in their enterprise architectures. Selecting solutions consistent with

an agency's technical reference model reduces costs and increases interoperability through reduced integration costs and increased standardization. Lastly, over time agencies may have unintentionally deployed redundant capabilities among which one or more could be phased out to achieve cost savings.

Figure 5 depicts one approach to analyzing capabilities. Outside the FEA SPP there are numerous system and program assessments that use common evaluation criteria across a wide set of capabilities. Consider the example of the FIPS PUB 199 security categorization. Each variation in need for confidentiality, integrity, and availability leads to a mandated baseline set of security controls.

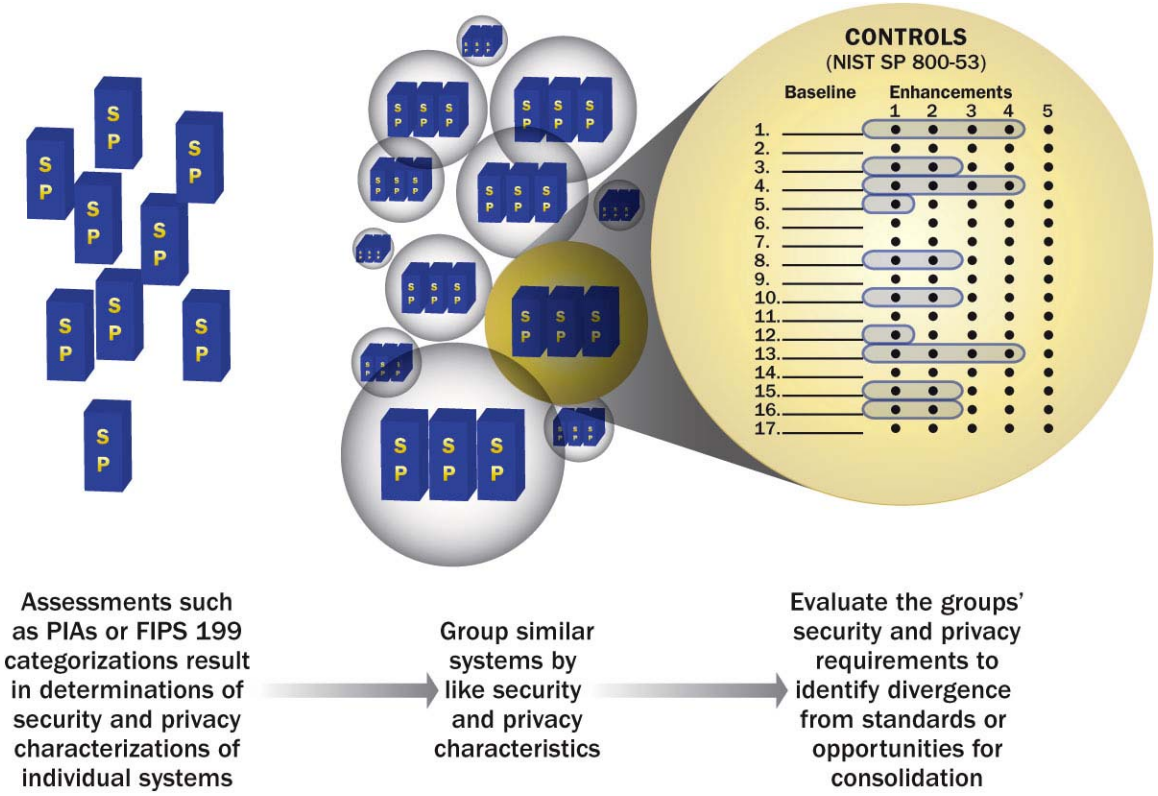

Figure 5. Analyze Capabilities

It follows that if multiple systems in an environment share the same security categorization, then they also share the same baseline security control requirements. Certification and accreditation assessments may reveal that, for any given control:

- Some systems will fail to exhibit the control,
- Some systems will have the independent capability to support the control, or
- Some systems may leverage a shared capability to support the control.

Aggregating FIPS PUB 199 security categorization results, or aggregating certification and accreditation results, may lead the FEA SPP implementation team to identify opportunities for standardizing or centralizing specific controls. This decision would

depend in part on the complexity and cost of the control. The provision of smart cards for identification and authentication is an example of a control that would be costly and inefficient to replicate across an agency.

Each of the analyses described above may identify a need to change existing or propose new capabilities as a solution to gaps or suboptimal capabilities. They both lead to the third analysis: a trade-off analysis of alternative solutions. This analysis recognizes that there are multiple solutions for each problem, and that each solution introduces different levels of residual risk and varying financial burdens. OMB directs agencies to consider alternative solutions and evaluate them based on functionality, risk, cost and interoperability. Alternatives are addressed through a series of trade-off analyses, resulting in a set of proposed investments that can be mapped to the agency's *to-be* architecture (see Figure 6).

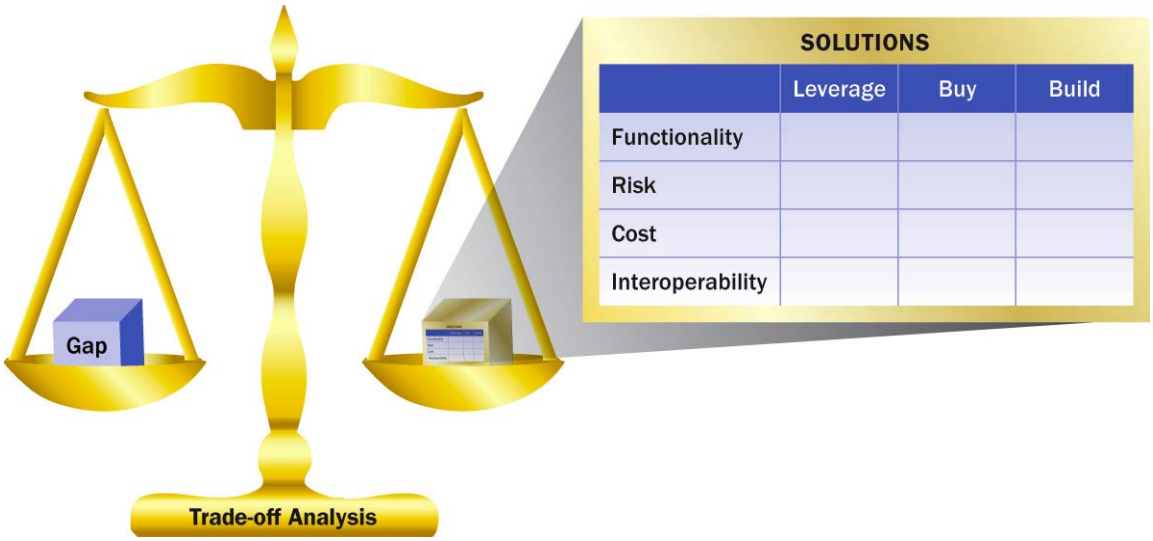

Figure 6. Analyze Trade-offs
The trade-off analysis supports the evaluation of alternatives and the selection of the capability that best meets Agency needs.

After accounting for the risks and benefits of alternatives, agencies should leverage an existing capability over buying a commercial solution. Similarly, purchasing commercial solutions is preferable to developing custom solutions. This is because leveraging is usually more cost-effective than purchasing a commercial solution, and purchasing a commercial solution is usually more cost effective than developing custom solutions. When agencies evaluate options for leveraging, they should consider solutions in their own agency as well as solutions from other agencies. Leveraging solutions across federal agencies is a goal of FEA efforts.

The results of the trade-off analysis support the investment prioritization process, both at the programmatic level and at the information technology investment review board

(ITIRB). Incorporation of the trade-off analysis in the business cases, and the references to the risk analyses and enterprise architecture content provide the basis for informed risk-based decision-making during the investment review, prioritization, and funding decisions.

3.2.2 Activities

The following activities support the goals and objectives of Stage I. For each activity, security and privacy information for the enterprise and/or program should be integrated into the agency's enterprise architecture. The following table provides a tool to determine where activities' outputs should be documented, identify the location where data is maintained, identify the owners of associated data, and document any corrective actions identified to improve the data or complete the activity.

Table 7. Stage II Activities

Goals, Objectives, Activities	EA Component	Information Location	Information Owner	Issues
A. 1. between current requirements and the current or planned capabilities to meet those requirements. Unmet requirements are then assessed to verify if they must be met to appropriately manage security and privacy risks. a. Identify the gap between requirements and capabilities. i. security and 17 privacy control families. In Stage I, the FEA SPP implementation team maps requirements and capabilities to the control families. Conduct a family-by-family assessment to identify requirements that are not supported by a specific capability. Subsequent activities in Stage II address unmet requirements.	Baseline, Transition Strategy[19], Target[20]			

[19] "Transition Strategy" is the plan for moving from the *as-is* architecture to the *to-be* architecture.

[20] "Target" is the *to-be* architecture.

Goals, Objectives, Activities	EA Component	Information Location	Information Owner	Issues
ii. Determine if unmet requirements are addressed in the agency's current future plans (through a review of the "target" architecture).	Transition Strategy, Target			
b. Assess the risks associated with gaps between requirements and capabilities. An accounting of security and privacy features is necessary to justify investments in OMB business cases[21].	Baseline, Transition Strategy, Target			
i. unmet requirement can be mitigated or accepted.				
ii. enterprise. Determine whether currently funded security and privacy capabilities address residual risks.	Baseline, Transition Strategy			
iii. *be* architecture.	Transition Strategy, Target			
iv. Stage II.	Transition Strategy, Target			
c. Document gaps in the enterprise architecture and FISMA Plan of Action & Milestones (POA&M). Enterprise-wide initiatives and/or critical security and privacy activities should be reflected in the agency's enterprise architecture transition strategy.	Baseline, Transition Strategy, Target			

[21] OMB A-11.

Goals, Objectives, Activities	EA Component	Information Location	Information Owner	Issues
2. Analyze Capabilities. Evaluate the overall capabilities portfolio to assess common risks, identifying opportunities for centralization and standardization. a. Aggregate program and system-level security and privacy assessments such as FIPS PUB 199 security characterizations and Privacy Impact Assessments. ▪ An agency with 100 systems may find that 50 are all subject to the Low/Low/Low security control baseline; another 25 may be subject to the High/High/Medium baseline; and the remaining 25 to an assortment of other combinations. ▪ An agency may determine that 30 of their systems hold personally identifiable information subject to the Privacy Act, HIPAA, or other privacy law considerations.	Baseline			
b. Evaluate the controls mandated for groups of systems. Use Stage I's mapping of requirements and capabilities to control families to assess current or planned capabilities.	Baseline, Transition Strategy, Target			
i. Identify opportunities to provide more effective and/or less expensive centralized security and privacy capabilities. Determine which controls are most complex or expensive to deploy at the system-level but which may be appropriate for an enterprise solution. ▪ NIST SP 800-53 summarizes required security control baselines and enhancements. ▪ Privacy laws and regulations establish a framework of appropriate privacy controls.	Baseline, Transition Strategy, Target			
ii. Identify capabilities that are inconsistent with common agency standards. Determine if standardizing those inconsistent capabilities on an agency standard will reduce security and privacy risk, increase interoperability, or reduce costs. For example, consider operating systems with similar security and privacy requirements for implementation within the same or similarly configured infrastructure.	Baseline, Transition Strategy, Target, TRM			

Goals, Objectives, Activities	EA Component	Information Location	Information Owner	Issues
iii. Identify capabilities not driven by a specific requirements. Capabilities may be identified through this assessment because their requirements have not been adequately captured in Stage I. If that is not the case, assess the need for the capability.	Baseline, Transition Strategy, Target			
B. 1. Informed risk-based decision making requires alternative analyses on sufficiency of the solution and associated costs and benefits managed to expectations for functionality. Criteria should include a review of all risk, benefit, and cost factors leading to selecting the most effective plan of action to address unsupported requirements.				
a. Evaluate the extent to which each alternative will meet the applicable security and privacy requirements and the extent to which they leave the agency exposed to residual risks.	Transition Strategy, Investment Portfolio			
b. Evaluate life cycle costs required to fund the investment or modification. If the alternative is already included in PO&AM, then use the costs from the POA&M in the analysis of the alternative. If not, then develop a cost estimate accounting for all life cycle costs associated with the alternative. All costs should also be risk-adjusted to account for foreseeable investment risks over the investment life cycle to facilitate comparison.	Transition Strategy, Investment Portfolio			
c. Evaluate the agency's inventory of approved technologies and services in the agency's TRM or TRM-equivalent to identify the preferred standards. Select solutions consistent with the agency's technical reference model. To reduce risks in the target environment, specific security and privacy investments may be needed in the technical and service infrastructures that are not addressed with the current security and privacy services and technologies.	Transition Strategy, Investment Portfolio, TRM			

Goals, Objectives, Activities	EA Component	Information Location	Information Owner	Issues
2. Evaluate gaps or capabilities to be improved and prioritize one or more to be addressed through an investment of new funds or realignment of existing resources. Whether addressing gaps at the programmatic or enterprise levels, ensure that enterprise needs are considered. Prioritize the selection based on: ▪ Breadth of impact across the enterprise ▪ Impact of the gap on the accomplishment of agency business ▪ Relevance of the gap to outstanding POA&M items. Addressing these items is important because agencies must report the status of POA&M corrective actions to OMB along with associated risks.	Transition Strategy, Investment Portfolio			
a. The analysis of alternatives evaluates the technically viable alternatives through a systematic paring down of the potential alternatives to feasible ones to the most viable alternatives. Viable alternatives are established by examining: ▪ The baseline environment and the requirements requiring attention ▪ Potential alternatives – those alternatives theoretically possible of addressing requirement needs ▪ Feasible alternatives – of the potential alternatives, those alternatives that can address the requirement needs given the constraints and limitations of the environment ▪ Viable alternatives – of the feasible alternatives, those alternatives that can be realistically implemented	Transition Strategy, Investment Portfolio			
b. Once feasible alternatives have been identified, an analysis of the costs, benefits, and risks of each viable alternative should be performed. OMB A-11 states that each prospective investment should include at least three alternatives (i.e., a baseline and at least two viable alternatives).	Transition Strategy, Investment Portfolio			
c. To make sound investment decisions, decision-makers must consider how cost, benefit, and risk interact.	Transition Strategy, Investment Portfolio			

Goals, Objectives, Activities	EA Component	Information Location	Information Owner	Issues
d. The most useful financial results in an investment decision appear in a time-based cash flow summary. This summary is used to describe the alternative solutions considered for mitigating the capability gap that the investment is expected to address. Each alternative should provide comparisons of the costs over time for each alternative.	Transition Strategy, Investment Portfolio			
3. internally deployed capabilities. a. Assess internally reusable capabilities. ▪ Stage I activities promote the identifying security and privacy capabilities and mapping those capabilities to control families and the agency enterprise architecture. There are unlikely to be any applicable internally reusable capabilities when Stage II activities immediately follow the completion of Stage I. However, over time Stages I and II will become somewhat disconnected. A quick scan of the control families and agency enterprise architecture may yield unexpected solutions. ▪ As part of this activity, evaluate the agency inventory of software licenses.	Baseline			
b. Research other agencies' solutions; many agencies have similar security and privacy challenges and some have capabilities available for reuse centrally registered at http://www.core.gov/. Other capabilities may be found through inquiries to OMB or other Federal agencies.				
c. Research opportunities for support through OMB's Information Systems Security Line of Business.				
d. Join or establish relevant communities of practice around specific unmet requirements to facilitate the creation of capabilities that are broadly applicable across the Federal government.[22]				

[22] http://www.et.gov/ is a growing Federal government resource that may contribute to the identification of communities of practice and associated shared capabilities.

Goals, Objectives, Activities	EA Component	Information Location	Information Owner	Issues
4. Identify opportunities to obtain capabilities from the marketplace. (i.e., commercial off the shelf solutions) other agencies and evaluate the opportunities for cross-agency re-use.				
5. components have been identified, comparisons can be made to the baseline and among the viable alternatives.	Transition Strategy, Investment Portfolio			
c.				
1. gap analysis and legacy capabilities analysis.	Baseline, Transition Strategy, Target			
2. business case formats.	Transition Strategy, Target			
3. ITIRB.	Transition Strategy			

3.3 Stage III – Selection

3.3.1 Introduction

Stage III is an enterprise evaluation of the solutions proposed in Stage II and the selection of major investments. In Stage III the FEA SPP implementation team works with the CFO and ITIRB to integrate outputs from previous stages into the agency-wide capital planning process to ensure:

- Evaluation of individual proposals so that each fully reflects the outputs of Stages I and II.
- Selection of individual proposals that best support the business, security, and privacy needs of the organization.
- Documentation of the updated to-be architecture and sharing of reusable components.

The CFO and ITIRB begin by evaluating all proposals using consistent criteria. Ideally, the Stage II trade-off analysis is consistent with the evaluation criteria. The CFO and ITIRB are then merely enforcing expectations articulated in enterprise architecture principles and OMB Exhibit 300 budget justification criteria.

While not every proposal from Stage II will be a major investment, all proposed solutions should undergo the executive review to ensure they meet Agency criteria and are consistent with the *to-be* architecture. As agencies investigate alternatives, they will seek to reuse solutions that may not require significant funding. However, these proposed solutions should still undergo the executive review to ensure they meet Agency criteria and are consistent with the *to-be* architecture.

Stage II promotes proposing solutions that are consistent with enterprise needs. Ultimately, it is the role and responsibility of the ITIRB to select a mix of proposals that optimizes business needs; maximizes available funds; and appropriately addresses confidentiality, integrity, availability, and privacy of the underlying federal information and federal information systems. This selection is made with consideration of the *as-is* and *to-be* architectures. ITIRBs may wish to prioritize proposals based on various agency needs; OMB promotes selecting shared or sharable capabilities over unique, non-shareable solutions.

Scarce resources will force the ITIRB to balance functional needs against security and privacy. In some cases an agency may prioritize funding for centralized security or privacy investment before investing in a functional capability that may lack needed security or privacy features. Risk mitigation strategies must be defined and implemented to address the residual risks from unfunded security and privacy aspects of investments. Risk mitigation strategies should feed back into Stages I and II because business processes and other aspects of the enterprise architecture may need to be changed to mitigate the security and privacy risks identified.

Once the CFO and ITIRB make their selection, the agency will have new capabilities to document and capture in the agency enterprise architecture. The new capabilities will

need to be reflected in the to-be architecture and the transition plan. Agencies will want to communicate results internally to ensure program offices and security and privacy stakeholders are aware of the new capabilities. Agencies should also consider publicizing externally leveragable capabilities registered at http://www.core.gov or available through OMB's Information Systems Security Line of Business (ISSLOB).[23]

[23] The ISSLOB addresses four areas: training, FISMA reporting, situational awareness and incident response, and security solutions. ISSLOB centers of excellence may be able to provide needed security-related services.

3.3.2 Activities

The following activities support the goals and objectives of Stage I. For each activity, security and privacy information for the enterprise and/or program should be integrated into the agency's enterprise architecture. The following table provides a tool to determine where activities' outputs should be documented, identify the location where data is maintained, identify the owners of associated data, and document any corrective actions identified to improve the data or complete the activity.

Table 8. Stage III Activities

Goals, Objectives, Activities	EA Component	Information Location	Information Owner	Issues
A. 1. proposals in a manner consistent with FEA SPP activities and based on the adequacy of security and privacy considerations.[24] a. Define minimally acceptable processes for assessing proposals.				
i. the five enterprise architecture reference models.	All reference models			
ii. the 17 security and 17 privacy control families.				
iii. the program selected the proposed option. The review of alternatives is an essential part of effective budget planning. Require program executives to incorporate the results of trade-off analyses into OMB and agency business cases to demonstrate informed risk-based decision-making and to comply with OMB and agency budget submission requirements.	Transition Strategy, Investment Portfolio[25]			

[24] ISO/IEC Standard 21827, *Systems Security Engineering – Capability Maturity Model,* provides guidance for defining processes and acceptable evidence.

[25] "Investment Portfolio" is an agency's collection of funded initiatives.

Goals, Objectives, Activities	EA Component	Information Location	Information Owner	Issues
iv. Require compliance with OMB or agency business case criteria.[26] This should include establishing an appropriate level of detail for security and privacy budget discussions.	Transition Strategy, Investment Portfolio			
b. Define acceptable evidence to support those processes.	Transition Strategy, Investment Portfolio			
c. Express a preference for leveraging existing capabilities.	Baseline			
2.	Transition Strategy, Investment Portfolio			
3.	Transition Strategy, Investment Portfolio			
B. 1. a. Consistency. Question and closely examine justifications for deviations from the agency's inventory of approved security and privacy-related technologies and services as described in the to-be architecture. Security and privacy controls that lay outside the current enterprise architecture are likely to be less effective, more expensive, and less interoperable. Consider whether the goals of such investments may be accomplished differently, within the context of the current enterprise architecture. Carefully weigh the implications of approving any deviation.	Baseline, Transition Strategy, Target, Investment Portfolio, TRM			

[26] OMB A-11.

Goals, Objectives, Activities	EA Component	Information Location	Information Owner	Issues
b. Necessity. Evaluate the need for new security and privacy capabilities. i. capability maps to one or more specific requirements and directly contributes to associated performance metrics.	Transition Strategy, Target, Investment Portfolio, PRM			
ii. new capability is necessary. New security and privacy capabilities should be designed to be leveragable beyond the immediate need.	Baseline, Transition Strategy, Target, Investment Portfolio			
c. Enterprise risk. Assess risks accepted through the proposed investment. Determine the impact that security and privacy choices may have on the broader enterprise.	Transition Strategy, Target, Investment Portfolio			
i. aspects of proposed investments. Unaddressed security and privacy requirements may impact other parts of the enterprise and other interconnected organizations.	Transition Strategy, Target, Investment Portfolio			
ii. requirements. The IRB and program executives must understand risks associated with underfunding of security and privacy requirements. Lack of investment into mitigating identified risks will increase overall risk to an agency.	Transition Strategy, Target, Investment Portfolio			
d. Cost. Assess the adequacy of security and privacy-related budget lines. i. OMB budget preparation guidance requires specific budget allocation for security management.	Transition Strategy, Investment Portfolio			

Goals, Objectives, Activities	EA Component	Information Location	Information Owner	Issues
ii. Evaluate the adequacy of specific funding for functional and compliance activities across the 17 security and 17 privacy controls. For example, do they include funding for mandated security and privacy assessments? Do they include funding to provide security and privacy awareness, training, and education?	Transition Strategy, Investment Portfolio			
iii. Determine if the agency can reduce costs by leveraging other initiatives or technologies and services used elsewhere in government, including leveraging specific services or the entire capability from other agencies.	Transition Strategy, Investment Portfolio			
2. requires all investments to have corresponding security budgets included and explicitly indicated in the budget, unless they satisfy the security or privacy component through another budget line item. Highlight shared security and privacy investments to ensure that they are funded. Otherwise, investments that depend upon them will not have sufficient security and privacy and may not be compliant. a. Assign highest priority to those proposed investments that provide central security and privacy capabilities.	Transition Strategy, Investment Portfolio			
b. Assign second highest priority to other IT investments that provide or leverage shared capabilities.	Transition Strategy, Investment Portfolio			
c. Assign lowest priority to IT investments that do not provide shared capabilities.	Transition Strategy, Investment Portfolio			
3. opportunities to reduce cost, increase functionality, and increase interoperability.	Baseline, Transition Strategy, Investment Portfolio			

Goals, Objectives, Activities	EA Component	Information Location	Information Owner	Issues
a. Identify opportunities to centralize capabilities—the senior agency officials for security and privacy should conduct a trade-off analysis to determine the best approach to centralizing capabilities.	Transition Strategy, Investment Portfolio			
b. Identify opportunities to appropriately reduce (but not eliminate) diversity of standards and approaches for accomplishing security and privacy objectives. Such changes may have a positive impact on security, privacy, interoperability, and cost, but should not be undertaken without careful consideration of the up-front costs, and especially the impact on accomplishing agency business objectives. Periodically assess the inventory of approved technologies and services to determine their sufficiency for the target architecture and/or new investment proposals.	Transition Strategy, Investment Portfolio, TRM			
4. budget. Highlight residual risks associated with unfunded proposals.				
C. 1. a. Update the *to-be* architecture after each budget cycle to reflect new investments and associated residual risks. The to-be architecture should portray the security and privacy features of the enterprise's mission and characterize its exposure to risks of the agency's enterprise architecture components.				
i. (e.g., privacy, medical, proprietary, financial, contractor sensitive, trade secret, investigation); and ii) information systems (e.g., mission critical, mission support, administrative).	Transition Strategy, Target			
ii. guidance in NIST SP 800-59, Guideline for Identifying an Information System as a National Security System.	Transition Strategy, Target			
iii. categories in accordance with FIPS PUB 199 and NIST SP 800-60.	Transition Strategy, Target, TRM, SRM			

Goals, Objectives, Activities	EA Component	Information Location	Information Owner	Issues
b. Update the enterprise transition plan after each budget cycle to reflect activities supporting new investments. Relate security and privacy funding request to agency Enterprise Architecture components including transition plans. Effective impact analyses to the enterprise as a whole will include architecture analyses. Investments are a component of the transition plan and may impact other ongoing or concurrent investment plans, as well as the ultimate target architecture. Ensure that the transition plan reflect risk mitigation for residual risks.	Transition Strategy			
c. Generate a report from the agency's enterprise architecture summarizing security and privacy features across each architecture component or reference model.				
i. The report should summarize key security and privacy drivers (including trust agreements established with external entities exchanging information) and enumerate the elements of the transition strategy that are funded to manage the security and privacy risks associated with fulfilling the mission of the agency.	Transition Strategy, Target			
ii. Use the report and the agency's enterprise architecture as a baseline for future FEA SPP iterations and with each update of the enterprise architecture and/or budget cycle.	Transition Strategy, Target			
2. a. The enterprise should ensure internal awareness of major security and privacy capabilities. Document and publicize available shared security and privacy capabilities with program developers responsible for implementing and maintaining business processes and systems. This may begin as an artifact of the agency enterprise architecture system. Outreach and publicity may provide valuable assistance to programmatic trade-off analysis efforts.	Transition Strategy, Target. All reference models			
b. The agency should consider promoting and sharing security and privacy capabilities with other Federal agencies. Publish sharable security and privacy capabilities to http://www.core.gov.	Transition Strategy, Target. All reference models			

4. Chapter Four: FEA SPP Implementation Over Time

This document describes the FEA SPP methodology as a three-step process of identifying requirements and capabilities, evaluating requirement gaps and current capabilities, and selecting investments that best support the enterprise. The discussion presented the methodology as a linear process with equal weight given to each stage. However, agency participants may find that actual implementation of the FEA SPP necessitates changes in emphasis over time (see Figure 7).

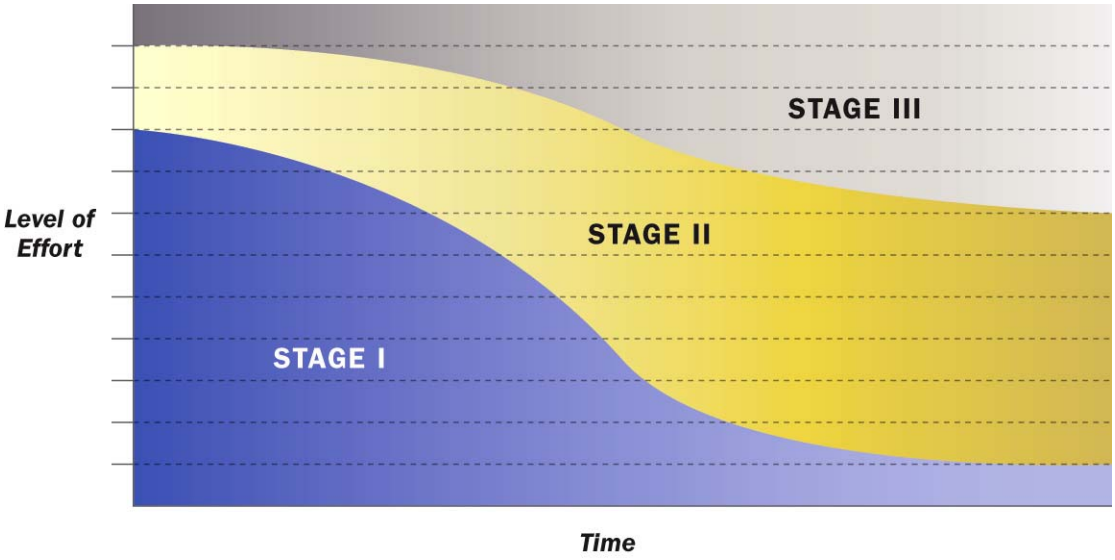

Figure 7. FEA SPP Implementation Level of Effort Over Time

Stage I addresses researching and documenting requirements and capabilities and capturing these in the agency enterprise architecture. In the initial implementation of the FEA SPP, agencies will likely find this to be a significant undertaking. However, effectively capturing requirements and capabilities in the enterprise architecture will prove critical to Stage II and III analyses. After the initial effort, the results of Stage I will be largely reusable with a moderate amount of maintenance. Agencies should consider conducting updates at least annually and also with the release of new requirements and as new capabilities are introduced or existing capabilities changed or retired.

Stage II consists of an analysis of potential capabilities to address a business need, an unmet security or privacy requirement, and current capabilities to identify opportunities for consolidation or improvement. Such analyses already take place outside the context of the FEA SPP; OMB A-11 requires presenting an alternative analysis that details the advantages and disadvantages of pursuing at least three viable alternatives to the status quo for major investments that warrant an Exhibit 300. The benefits of Stage II activities are in identifying a more complete set of alternatives and also in the consistent documentation of those alternatives. Over time, Stage II activities will become simpler and less time-consuming as a result of Stage I and III activities. Stage II efforts may also shift from closing gaps to optimization over time.

Stage III focuses on an agency's ITIRB. This stage promotes requirements for complete documentation of security and privacy alternatives and costs in each investment submission. It encourages preferences for investments that are consistent with the current architecture and which leverage existing security and privacy components. It also encourages an evaluation of program-level investments to identify opportunities for more efficient and effective completion of security and privacy objectives. Initially, Stage III may only require a modest effort. Many of the activities described necessitate more information than will be readily available. However, as agencies document security and privacy requirements and capabilities more fully, they will enable Stage III benefits.

The FEA SPP provides an opportunity for agencies to take an enterprise perspective of security and privacy and establish processes to identify requirements, leverage capabilities, and manage investments effectively. As agencies implement the FEA SPP, they will find opportunities to share resources and capabilities across domains, programs, and agencies.

Appendix A. References

Laws

Clinger Cohen Act of 1996. (Clinger Cohen Act)

E-Government Act of 2002. (E-Gov Act)

Federal Acquisition Streamlining Act of 1994. (FASA)

Federal Information Security Management Act of 2002. (FISMA)

Health Insurance Portability and Accountability Act of 1996. (HIPAA)

Privacy Act of 1974. (Privacy Act)

Executive Policy

OMB Circular A-11, *Preparation, Submission, and Execution of the Federal Budget,* November 2005. (OMB A-11)

OMB Circular A-130, *Management of Federal Information Resources*, November 2000. (OMB A-130)

OMB Memorandum 03-22, *Guidance on Implementing the Privacy Provisions of the E-Government Act of 2002,* September 2003. (M-03-22)

OMB Memorandum 05-15, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, June 2005. (M-05-15)

Federal Standards

FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, U.S. Department of Commerce, December 2003

FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*, U.S. Department of Commerce, March 2006.

International Standards

ISO/IEC Standard 21827:2002, *Systems Security Engineering – Capability Maturity Model*, October 2002.

Guidance

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, February 2005.

NIST SP 800-55, *Security Metrics Guide for Information Technology System*, July 2003.

NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004.

Other Resources

"Component Organization and Registration Environment," http://www.core.gov, April 2006.

"EmergingTechnology.gov," http://www.et.gov, April 2006.

Federal Enterprise Architecture Reference Model Maintenance Process, Chief Information Officer Council, et. al., June 2005.

FY07 Budget Formulation: FEA Consolidated Reference Model Document, OMB, May 2005.

GAO Report: Practical Guide to Federal Enterprise Architecture – Chief Information Officer Council Version 1.0 February 2001.
http://www.gao.gov/bestpractices/bpeaguide.pdf

A Practical Guide to Federal Enterprise Architecture Version 1.0., Chief Information Officer Council, February 2001.

Appendix B. Definitions

Table 9. Definitions

Term	Definition
Acceptable Use	Ensuring that personal information is used only in the manner provided on the notice, to which the individual consented, and in accordance with the publicly disclosed practices
Access Control	Limiting information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems), and to types of transactions and functions that authorized users are permitted to exercise
Accuracy of Data	Ensuring that personal information is accurate, particularly if harm or denial of benefits may result
Assigned Roles, Responsibilities, and Accountability	Identifying general and specific roles and responsibilities for the management and use of personal information and ensuring accountability for meeting these responsibilities
Audit and Accountability	Creating, protecting, and retaining information system audit records that are needed for monitoring, analyzing, investigating, and reporting unlawful, unauthorized or inappropriate information system activity, and ensuring that the actions of individual users can be traced so that the individual users can be held accountable for their actions
Authorization	Ensuring that all new and secondary uses of personal information not previously identified on the original collection notice are authorized by the individual
Availability	"Ensuring timely and reliable access to and use of information." (FISMA)
Awareness and Training	Ensuring that managers and users of information systems are made aware of the security risks associated with their activities and of applicable laws, policies, and procedures related to security, and ensuring that personnel are trained to carry out their assigned information security-related duties
Business Reference Model	"Function-driven framework used to describe the lines of business and sub-functions performed by the Federal government independent of the agencies that perform them. IT investments are mapped to the BRM to identify collaboration opportunities. (Exhibit 300)"
Capital Planning and Investment Control	"Decision-making process for ensuring that IT investments integrate strategic planning, budgeting, procurement, and the management of IT in support of agency missions and business needs. The term comes from the Clinger-Cohen Act of 1996 and generally is used in relationship to IT management issues" (Exhibit 300)
Certification and Accreditation and Security Assessments	Assessing security controls for effectiveness, implementing plans to correct deficiencies and to reduce vulnerabilities, authorizing the operation of information systems and system connections, and monitoring system security controls
Chain of Trust	Establishing and monitoring third-party agreements for handling personal information
Confidentiality	"Reserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information availability." (FISMA)

Term	Definition
Configuration Management	Establishing baseline configurations and inventories of systems, enforcing security configuration settings for products, monitoring and controlling changes to baseline configurations and to components of systems throughout their system development life cycles
Consent	Gaining consent for, and providing choices to, the individual to use their personal information
Contingency Planning	Establishing and implementing plans for emergency response, backup operations, and post-disaster recovery of information systems
Control	A safeguard or countermeasures that promote security or privacy objectives
Control Family	A group of related controls
Data Reference Model	"Framework used to promote the common identification, use, and appropriate sharing of data/information across the Federal Government. It provides standards and guidelines to help agencies structure, categorize, exchange, and manage their data to improve the ability of Government to perform cross-agency information sharing" (Exhibit 300)
Education: Awareness and Role-based Training Programs	Ensuring managers and users of personal information are made aware of the privacy risks associated with their activities and of applicable laws, policies, and procedures related to privacy
Exhibit 300	Part 7 (Section 300) of OMB Circular No. A-11. The Exhibit 300 provides the budget justification for major IT investments. For IT, this is a companion section to section 53. The policy and budget justification and reporting requirements in the Exhibit 300 apply to all agencies of the Executive Branch of the Government subject to Executive Branch review. An Exhibit 300 must be submitted for all major investments in accordance with this section. Major IT investments also must be reported on your agency's Exhibit 53.
Exhibit 53	(Part 53) of OMB Circular No. A-11. The Agency Exhibit 53 is the Agency IT Investment Portfolio and provides the total IT and information security spending for the year.
Federal Enterprise Architecture	A business-based framework for government-wide improvement. It describes the relationship between business functions and the technologies and information that support them. The FEA is being constructed through a collection of interrelated "reference models" designed to facilitate cross-agency analysis and the identification of duplicative investments, gaps, and opportunities for collaboration within and across federal agencies. (OMB Circular A-11, Part 7)
Identification and Authentication	Identifying and authenticating the identities of users, processes, or devices that require access to information systems
Incident Response	Establishing operational incident handling capabilities for information systems, and tracking, documenting, and reporting incidents to appropriate officials
Individual Rights	Providing individuals an opportunity to access and correct their personal information and to seek redress for privacy violations

Term	Definition
Integrity	"Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity" (FISMA)
Maintenance	Performing periodic and timely maintenance of systems, and providing effective controls on the tools, techniques, mechanisms, and personnel that perform system maintenance
Media Protection	Protecting information in printed form or on digital media, limiting access to information to authorized users, and sanitizing or destroying digital media before disposal or reuse
Minimum Necessary	Collecting the minimum amount of personal information necessary to accomplish the business purpose
Monitoring and Measuring	Monitoring the implementation of privacy controls and measuring their efficacy
Notice	Providing notice to the individual of the information practices, such as the acceptable uses, before collecting personal information
Performance Reference Model	"Standardized performance measurement framework used to characterize performance in a common manner where necessary. The PRM helps agencies produce enhanced performance information; improve the alignment and better articulate the contribution of inputs, such as technology, to outputs and outcomes; and identify improvement opportunities that span traditional organizational boundaries." (Exhibit 300)
Personnel Security	Ensuring that individuals in positions of authority are trustworthy and meet security criteria, ensuring that information and information systems are protected during personnel actions, and employing formal sanctions for personnel failing to comply with security policies and procedures
Physical and Environmental Protection	Limiting physical access to systems and to equipment to authorized individuals, protecting the physical plant and support infrastructure for systems, providing supporting utilities for systems, protecting systems against environmental hazards, and providing environmental controls in facilities that contain systems
Planning	Developing, documenting, updating, and implementing security plans for systems
Policies and Procedures	Creating policies and procedures governing the appropriate use of personal information and the implementation of privacy controls
Privacy	"The appropriate use of personal information." (International Association of Privacy Professionals) https://www.privacyassociation.org/
Privacy as Part of the Development Life Cycle	Implementing privacy reviews and controls throughout the system development life cycle
Public Disclosure	Publicly disclosing privacy policies and procedures for a program or system
Reporting and Response	Providing senior managers and oversight officials the results of the monitoring and measuring of privacy controls and responding to privacy violations

Term	Definition
Risk Assessment	Assessing the risk to organizational operations, assets, and individuals resulting from operating information systems, and processing, storing, or transmitting information
Risk Management	Assessing and managing risks to operations, assets, and individuals resulting from collecting, sharing, storing, transmitting, and using personal information
Security	Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability (FISMA)
Security Measures	Implementing the appropriate safeguards to ensure the appropriate confidentiality, integrity and availability of personal information
Services-Component Reference Model	"Common framework and vocabulary used for characterizing the IT and business components that collectively comprise an IT investment. The SRM helps agencies rapidly assemble IT solutions through the sharing and re-use of business and IT components. A component is a self-contained process, service, or IT capability with pre-determined functionality that may be exposed through a business or technology interface." (Exhibit 300)
System and Communications Protection	Monitoring, controlling and protecting communications at external and internal boundaries of information systems, and employing architectural designs, software development techniques, and systems engineering principles to promote effective security
System and Information Integrity	Identifying, reporting, and correcting information and system flaws in a timely manner, providing protection from malicious code, and monitoring system security alerts and advisories
System and Services Acquisition	Allocating resources to protect systems, employing system development life cycles processes, employing software usage and installation restrictions, and ensuring that third-party providers employ adequate security measures to protect outsourced information, applications, or services
Technical Reference Model	"Foundation used to describe the standards, specifications, and technologies supporting the delivery, exchange, and construction of business (or service) components and E-Gov solutions. The TRM unifies existing agency TRMs and E-Gov guidance by providing a foundation to advance the re-use of technology and component services from a government-wide perspective." (Exhibit 300)

Appendix C. Acronyms

BRM	Business Reference Model
CFO	Chief Financial Officer
CIO	Chief Information Officer
DRM	Data Reference Model
FASA	Federal Acquisition Streamlining Act of 1994
FEA	Federal Enterprise Architecture
FEA SPP	Federal Enterprise Architecture Security and Privacy Profile
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Management Act of 2002
HIPAA	Health Insurance Portability and Accountability Act of 1996
ISSLOB	Information Systems Security Line of Business
IG	Inspector General
IT	Information Technology
ITIRB	Information Technology Investment Review Board
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
POA&M	Plan of Action and Milestones
PRM	Performance Reference Model
SRM	Service-Component Reference Model
TRM	Technology Reference Model

Appendix D. Privacy Requirements

As part of developing the FEA SPP, 17 unique privacy controls were identified. Table 10 provides an initial set of privacy requirements grouped into the appropriate privacy control areas. These privacy requirements are meant to begin the discussion on privacy for Stage I. This set of requirements is not exhaustive but rather a representative set. Agencies will need to enhance this initial list with requirements from additional drivers applicable to their agency. The requirements identified here apply to most Federal agencies.

Table 10. Partial List of Privacy Requirements

Control Area	Requirement	Reference	Citation
Policies and Procedures	Establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record.	Privacy Act	5 U.S.C. §552a(e)(9)
	Promulgate rules to ensure compliance with the requirements of the Privacy Act.	Privacy Act	5 U.S.C. §552a(f) (1) -(5)
	Have a written process documenting the process for conducting and reviewing privacy impact assessments.	M-05-15	Attachment, Section D. B. Practices and Procedures
	Have a policy for the use of tracking technologies on websites.	M-03-22	Attachment A. III. Privacy Policies on Agency Websites
	Write clear, easy to understand privacy policies for website practices and post on websites.	M-03-22	Attachment A. III. Privacy Policies on Agency Websites
Privacy in the Developmental Life Cycle	Agencies must perform and update privacy impact assessments when system changes create new privacy risks.	M-03-22	Attachment A. II. Privacy Impact Assessment
	Business cases in the Exhibit 300s will be evaluated according to how well security and privacy details of the investment are documented and budgeted for throughout the life cycle.	OMB A-11	Part 7, Section 300.10

Control Area	Requirement	Reference	Citation
Assigned Roles and Responsibilities	Agencies must identify a senior agency official for privacy who is responsible for agency privacy compliance activities (privacy policy as well as IT policy), evaluations of the privacy impact of legislative, regulatory, and other policy proposals and assesses the impact of technology of personal information, and technologies that allow for continuous auditing of compliance with stated privacy policies and practices.	M-05-15	Section D. A. Privacy Official Responsibilities
	Agencies must establish a Data Integrity Board to oversee and coordinate the components of and implementation of matching programs consistent with the Privacy Act as Amended.	Privacy Act	5 USC 552a(u)(2)-(5)
	All Federal employees and contractors must remain mindful of privacy and their obligation to protect information in identifiable form.	M-03-22	Attachment A VI.
Assigned Roles and Responsibilities	Implementing the Privacy Provisions of the E-Government Act requires the cooperation and coordination of privacy, security, FOIA/Privacy Act, and project officers located in disparate organizations with agencies. Clear leadership and authority are essential.	M-03-22	Attachment A VI.
	Head of each agency shall have primary responsibility for managing agency information resources.	OMB A-130	9.a. Assignment of Responsibilities
	Agencies must identify those individuals in the agency (e.g., information technology personnel, Privacy Act Officers) that have day-to-day responsibility for implementing section 208 of the E-Government Act, the Privacy Act, or other privacy laws and policies; designate an appropriate senior official or officials (e.g., CIO, Assistant Secretary) to serve as the agency's principal contact(s) for information technology/web matters and for privacy policies. The designated official(s) shall coordinate implementation of OMB web and privacy policy and guidance; and designate an appropriate official (or officials, as appropriate) to serve as the "reviewing official(s)" for agency PIAs.	M-03-22	Attachment A VI.

Control Area	Requirement	Reference	Citation
Public Disclosure	For all systems of records publish a notice in the Federal Register that includes the categories of individuals on whom records are maintained in the system, the categories of records maintained in the system; each routine use of the records contained in the system, including the categories of users and the purpose of such use; the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records; the title and business address of the agency official who is responsible for the system of records; the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him; the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining; to him contained in the system of records, and how he can contest its content; and the categories of sources of records in the system.	Privacy Act; OMB A-130	5 U.S.C. §552a(e)(4); Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals
	Make the PIA publicly available.	M-03-22	Attachment A.3 PIA Review and Publication
Notice	Inform individuals at the time of collection and on the collection media of the authority which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary; the purpose(s) of the information collection; the routine uses; and the effects of not providing all or part of the requested information.	Privacy Act	5 U.S.C. §552a(e)(3)
	Make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record.	Privacy Act	5 U.S.C. §552a(e)(8)
	Adopt machine-readable technology that alerts users automatically about whether site privacy practices match their personal privacy preferences. Such technology enables users to make an informed choice about whether to conduct business with that site.	M-03-22	Attachment A. IV. Privacy Policies in Machine-Readable Formats

Control Area	Requirement	Reference	Citation
Consent	Do not disclose any record that is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be subject to one of the 12 exceptions.	Privacy Act	5 U.S.C. §552a(b)
Education and Awareness	Instruct each person involved with a system of records on the rules of conduct and penalties for noncompliance.	Privacy Act	5 U.S.C. §552a(e)(9)
	Inform and educate employees and contractors of their responsibility for protecting information in identifiable form.	M-03-22	Attachment A VI.
	Ensure that all agency personnel are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure.	M-05-15	Section D B. Procedures and Practices
	Provide job-specific information privacy training (i.e., detailed training for individuals directly involved in the administration of personal information or information technology systems, or with significant information security responsibilities).	M-05-15	Section D B. Procedures and Practices
Security Measures	Establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records.	Privacy Act	5 U.S.C. §552a(e)(10)
	Ensure PIA identifies how the information will be secured (administrative and technical controls).	M-03-22	Attachment A.II.C. Conducting a PIA
Minimum Necessary	Maintain in records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive order of the President.	Privacy Act	5 U.S.C. §552a(e)(1)
Acceptable Use	An individual's name and address may not be sold or rented by an agency unless such action is specifically authorized by law. This provision shall not be construed to require the withholding of names and addresses otherwise permitted to be made public.	Privacy Act	5 U.S.C. §552a(n)
Data Accuracy	Take reasonably necessary actions to ensure that records used to make determinations about an individual are accurate to assure fairness.	Privacy Act	5 U.S.C. §552a(e)(5)

Control Area	Requirement	Reference	Citation
	Prior to disseminating any record about an individual make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes.	Privacy Act	5 U.S.C. §552a(e)(6)
Individual Rights/ Individual Participation	Do not disclose any record that is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be subject to one of the 12 exceptions.	Privacy Act	5 U.S.C. §552a(b)
	Upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system.	Privacy Act	5 U.S.C. §552a(d)(1)
	Collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs.	Privacy Act	5 U.S.C. §552a(e)(2)
	Permit the individual to request amendment of a record pertaining to him and make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official.	Privacy Act	5 U.S.C. §552a(d)(2)
	Individual access may be declined if information is compiled in reasonable anticipation of a civil action or proceeding.	Privacy Act	5 U.S.C. §552a(d)(5)
	Inform any person or other agency about any correction or notation of dispute made by the agency of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.	Privacy Act	5 U.S.C. §552a(c) (1) (2) (3) (4)
	Maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity.	Privacy Act	5 U.S.C. §552a(e)(7)

Control Area	Requirement	Reference	Citation
Risk Management	Conduct a privacy impact assessment to analyze of how information is handled: to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.	M-03-22	Attachment A.II
	Ensure investment costs cover the life of each system and include all budgetary resources (direct appropriation, working capital fund, revolving funds, etc.). Life cycle costs should also be risk adjusted to include any risks addressed on the Capital Asset Plan and Business Case that have not been mitigated. Examples of areas that may cause the adjustment of life cycle costs would be strategic risks, technological risks, human capital issues, acquisition strategy, IT security and privacy risks, enterprise architecture, and any other issues identified on the capital asset plan.	OMB A-11	Part 2, Section 53.1
Authorization	No record that is contained in a system of records may be disclosed to a recipient agency or non-Federal agency for use in a computer matching program except pursuant to a written agreement between the source agency and the recipient agency or non-Federal agency.	Privacy Act	5 U.S.C. §552a(o)(1)
Chain of Trust	When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. Any such contractor and any employee of such contractor shall be considered to be an employee of an agency.	Privacy Act	5 U.S.C. §552a(m)
	No source agency may disclose any record which is contained in a system of records to a recipient agency or non-Federal agency for a matching program if such source agency has reason to believe that the requirements of subsection (p), or any matching agreement entered into pursuant to subsection (o), or both, are not being met by such recipient agency.	Privacy Act	5 U.S.C. §552a(q)(1)

Control Area	Requirement	Reference	Citation
	No source agency may renew a matching agreement unless the recipient agency or non-Federal agency has certified that it has complied with the provisions of that agreement; and the source agency has no reason to believe that the certification is inaccurate.	Privacy Act	5 U.S.C. §552a(q)(2)
Monitoring and Measuring	Conduct and be prepared to report the results of the following reviews of activities mandated by the Privacy Act including Section M Contracts, records practices, routine uses, exemptions, matching programs, training, violations and systems of records.	M-05-15	Section D. B. Procedures and Practices
	Review and document compliance with information privacy laws, regulations and policies.	M-05-15	Section D, C. Compliance Audits
	Document corrective action planned, in progress or completed to remedy identified compliance deficiencies.	M-05-15	Section D, C. Compliance Audits
	Provide the agency Inspector General (IG) with a compilation of privacy and data protection policies and procedures; summary of the agency's use of information in identifiable form and verification of intent to comply with agency policies and procedures.	M-05-15	Section D, C. Compliance Audits
	Business cases and budget estimates should reflect a commitment to privacy and should include a description of your privacy practices and steps taken to ensure compliance with all OMB privacy policies as set forth in OMB Memorandum 03-02 (September 26, 2003) and OMB Circular A-130, Appendix 1.	OMB A-11	Part 2, Section 31.8
Reporting and Response	Privacy compliance reporting has been consolidated into a single annual report, the Privacy Management Report included with FISMA reporting (in FY05).	M-05-15	All